SEGURANÇA dos SISTEMAS de INFORMAÇÃO

Gestão Estratégica da Segurança Empresarial

Pedro Tavares Silva
Hugo Carvalho
Catarina Botelho Torres

CENTROATLANTICO.PT

€22,20

€19,70

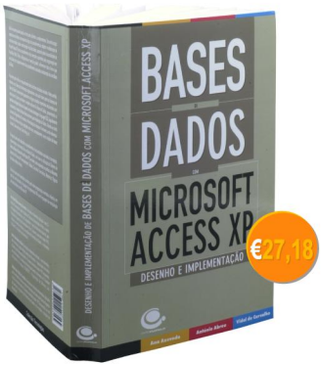
€27,18

€22,20

€24,69

€22,20

€22,20



€27,18

€27,18

Nota de Encomenda

Pode ser fotocopiada

Dirija as suas encomendas para: Centro Atlântico - Ap. 413 - 4764-901 V. N. de Famalicão

TÍTULO	Preço Unitário	Quant.	Sub-total

Total: € ☐☐☐,☐☐

SIM, desejo receber os títulos que assinalei sem qualquer despesa de envio.

☐ Envio cheque/Vale nº _____ à ordem do Centro Atlântico.

☐ Prefiro que debitem no meu cartão de crédito:

Número do cartão de crédito ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Cartão em nome de _____

Últimos três dígitos nas costas do Cartão: ☐☐☐ Validade: ☐☐☐☐ ☐ Mastercard ☐ Visa ☐ American Express

Empresa _____

Nome _____

Morada _____

CP ☐☐☐☐–☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Tel. ☐☐☐☐☐☐☐☐☐

E-Mail _____ Contribuinte ☐☐☐☐☐☐☐☐☐

Sem despesas de envio. As encomendas directas ao Centro Atlântico, para Portugal, não pagam custos de portes. Envios à cobrança são onerados em €2,5 por encomenda. Envios internacionais são onerados em €5.

Os dados recolhidos são processados automaticamente, sendo o seu fornecimento facultativo.

É garantido, nos termos da Lei, o direito de acesso e de rectificação bem como de não divulgação a terceiros, devendo dirigir-se para tal ao Centro Atlântico. Se não desejar receber informações sobre os nossos produtos e serviços assinale aqui com uma cruz ☐

Todos os preços já incluem IVA à taxa em vigor.

CENTROATLANTICO.PT

Apartado 413
4764-901 V. N. Famalicão

Rua da Misericórdia, 76
1200-273 Lisboa

Tel.: 808 20 22 21
geral@centroatlantico.pt

PEDRO TAVARES SILVA

HUGO CARVALHO

CATARINA BOTELHO TORRES

SEGURANÇA

DOS

SISTEMAS DE INFORMAÇÃO

Gestão Estratégica da Segurança Empresarial

Portugal/2003

Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial

Colecção: Sociedade da Informação
Autores: Pedro Tavares Silva, Hugo Carvalho e Catarina Botelho Torres

Direcção gráfica: Centro Atlântico
Revisão final: Centro Atlântico
Capa: Paulo Buchinho

Av. Dr. Carlos Bacelar, 968 - Escr. 1 - A
4764-901 V. N. Famalicão
Rua da Misericórdia, 76 - 1200-273 Lisboa
Portugal
Tel. 808 20 22 21

geral@centroatlantico.pt
www.centroatlantico.pt

Design e Paginação: Centro Atlântico

Impressão e acabamento: Rolo & Filhos
1ª edição: Abril de 2003
ISBN: 972-8426-66-6
Depósito legal: 193.992/03

Agradecimentos

Este e qualquer outro trabalho meu será sempre dedicado à Paula, ao Kukas e ao Kikas, pela extraordinária generosidade dela, que criou todo o tempo empregue neste projecto, e pela permanente e infinita compreensão, afecto e apoio de todos eles.

Pedro

À Filipa e ao Gugas, por tudo, ao Pedro pela energia e incentivo, e ao Fernando Almeida pela inspiração.

Hugo

Ao Nuno, à minha Mãe, à amiga Odete e em especial ao Diogo o meu pequenote, por todo o apoio e carinho que me permitiram participar neste projecto tão aliciante.

Catarina

Ao Rui São Pedro, Lisete Figueiredo, Manuel Lopes Rocha, Carlos Tomaz, Sandra Raimundo e Frederico Martins, muito obrigado por toda a disponibilidade e empenho demonstrados.

Os Autores

ÍNDICE

Introdução

O livro que tem em mãos introduz uma visão estratégica que lhe irá permitir encarar de forma integrada a segurança dos sistemas de informação da sua Empresa, considerando tanto o seu ponto de vista pessoal (quer seja técnico, de gestão ou outro) como as necessidades do negócio e a especificidade de todas as áreas técnicas inevitavelmente envolvidas.

Com esta obra espera-se transmitir a mensagem de que a segurança, mais do que um simples produto ou tecnologia que se pode adquirir, aplicar e esquecer, mais do que um comprimido (tecnológico ou monetário) supressor de sintomas, é um processo contínuo e abrangente, com implicações em todas as áreas empresariais, desde a Administração aos colaboradores que executam as operações quotidianas mais elementares. É um processo em permanente evolução, mutação e transformação, que requer um esforço constante para o seu sucesso e uma forte capacidade para provocar e gerir mudanças, tanto nos hábitos instituídos como na infra-estrutura de suporte da organização.

Como matéria transversal que é, a segurança deve envolver todos os níveis da Empresa e ser encarada como um facilitador dos processos e como forma de aumentar os níveis de confiança internos e externos. É este o grande argumento sobre o qual qualquer organização poderá capitalizar o seu investimento nesta área. Ao implementar este programa, estará a transmitir uma imagem de preocupação nesta matéria, cada vez mais importante e com maior visibilidade, conseguindo simultaneamente gerir o risco a que se encontra sujeita. O programa de segurança serve, deste modo, vários objectivos: a criação de uma base de protecção e confiança sobre a qual é desenvolvida uma actividade; um sinal claro e inequívoco de que a organização tem preocupações fundamentais com a integridade e preservação dos seus activos (quer sejam processos, produtos,

informação ou outros); a afirmação pública de dedicação de um cuidado particular aos interesses de parceiros, clientes ou fornecedores. São estes os resultados visíveis de quaisquer esforços neste campo.

É igualmente nestes factores que reside a força do argumento da segurança como opção estratégica e não apenas técnica ou tecnológica, com impacto positivo e inegável sobre a Empresa. Este livro pretende introduzir esta disciplina como um acto de gestão a curto, médio e longo prazo, no qual tem origem a alteração de processos e meios, de forma apontada às necessidades do negócio. Deste modo, o que se pretende é que o leitor olhe para além da sua área de conhecimento e reconheça a necessidade de trabalhar continuamente a segurança, onde quer que ela seja precisa, de uma forma uniforme. Também aqui se pretende que o leitor olhe para além das medidas de segurança que tem ao seu dispor, encarando-as como ferramentas para atingir um objectivo: importa, então, considerar o resultado e não apenas as medidas. A tecnologia serve para um objectivo, não sendo nunca um fim em si mesma.

A criação de um programa de segurança é, então, um criterioso alinhamento de prioridades, um cuidadoso equilibrar dos mais variados factores, um exercício de abrangência e um processo negocial que, garantidamente, requer tempo, perserverança, bastante paciência e capacidade para atingir compromissos e gerir o nível de segurança percebido pelos nossos diversos clientes, dos internos aos externos.

Pretende-se aqui apresentar um manual de referência para todos aqueles que, independentemente do seu grau de conhecimento técnico, têm de lidar com a segurança empresarial. Este é um livro escrito para todos os profissionais das áreas das tecnologias e sistemas de informação, responsáveis de segurança, directores, gestores ou chefes de departamentos técnicos ou de outras áreas do negócio, de programas ou projectos com componentes TI, bem como para consultores de segurança, responsáveis por informação crítica e para todos os que se encontrem de alguma forma envolvi-

dos na definição, implementação e gestão de medidas de segurança empresarial. Nas próximas páginas irá encontrar um "canivete suíço", contendo as ferramentas necessárias para a gestão estratégica da segurança, um manual de instruções para a resolução do vasto puzzle que é a segurança empresarial.

Este livro inicia-se com uma base teórica, abordando de seguida um conjunto de questões mais práticas, que estarão inevitavelmente presentes em qualquer agenda empresarial. Assim, na primeira parte deste livro são introduzidos e desenvolvidos temas como a teoria da segurança, gestão do risco ou áreas da segurança, que constituem a base sobre a qual é construído um Programa de Segurança Empresarial. Na segunda parte, a abordagem é mais pragmática, apresentando-se propostas para a criação, implementação e gestão das várias facetas da segurança, chamando a atenção para alguns obstáculos existentes ao longo do caminho e, sempre que possível, fornecendo indicações para os superar.

A tarefa de criação, implementação e gestão de um programa de segurança não é seguramente fácil. À primeira vista poderão existir enormes dificuldades, oposições internas ou problemas extremamente complexos cuja eliminação aparente ser praticamente impossível. Mas é neste elaborado processo de construção de um novo edifício, chamado “segurança”, que se encontra o grande desafio e o gozo de o superar.

Esperamos sinceramente que este livro o ajude levar a segurança à sua empresa.

Os Autores

Capítulo I - Teoria da Segurança

A segurança dos sistemas de informação (SI) engloba um número elevado de disciplinas que poderão estar sob a alçada de um ou vários indivíduos. Entre estas disciplinas encontram-se as seguintes:

- segurança de redes;
- segurança física;
- segurança de computadores;
- segurança do pessoal;
- segurança aplicacional;
- criptografia;
- gestão de projectos;
- formação;
- conformidade.

Neste primeiro capítulo iremos abordar alguns conceitos, princípios e modelos elementares da segurança dos SI, por forma a identificar uma base teórica de referência comum às diversas disciplinas, que permita a definição de um programa de prevenção e protecção equilibrado.

Princípios de Prevenção e Protecção

A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes são também utilizadas como forma de garantir a autenticidade e o não repúdio.

Todas estas medidas, independentemente do seu objectivo, necessitam ser implementadas antes da concretização do risco, ou seja, antes do incidente ocorrer. As medidas de segurança podem ser classificadas, em função da maneira como abordam as ameaças, em duas grandes categorias: prevenção e protecção.

A prevenção é o conjunto das medidas que visam reduzir a probabilidade de concretização das ameaças existentes. O efeito destas medidas extingue-se quando uma ameaça se transforma num incidente.

A protecção, por seu lado, é o conjunto das medidas que visam dotar os sistemas de informação com capacidade de inspecção, detecção, reacção e reflexo, permitindo reduzir e limitar o impacto das ameaças quando estas se concretizam. Naturalmente, estas medidas só actuam quando ocorre um incidente.

Exemplo: a vasta maioria das empresas implementa algumas actividades de prevenção contra incêndio, tais como a proibição de fumar em locais de risco (por exemplo, locais onde são armazenadas matérias inflamáveis) e actividades de protecção, tais como a disponibilização de extintores, para o caso de se iniciar um incêndio.

Um Programa de Segurança bem estruturado deverá reduzir as vulnerabilidades dos sistemas de informação e fazer evoluir as suas capacidades de inspecção, detecção, reacção e reflexo, assentando num conjunto universal de princípios que garanta o seu equilíbrio e eficiência.

Os princípios da segurança são, então, os seguintes:

- relação custo/benefício;
- concentração;
- protecção em profundidade;
- consistência do plano;
- redundância.

Procuraremos em seguida descrever estes princípios.

Relação Custo/Benefício

A relação custo/benefício traduz a necessidade de garantir uma relação favorável entre os gastos associados à implementação de medidas de segurança e o retorno em matéria de prevenção e protecção.

Embora assente no senso comum, este princípio é frequentemente esquecido, sendo normalmente considerados apenas os custos ou os benefícios isoladamente. Mais adiante, no capítulo "Gestão do Risco", serão abordadas as fórmulas que permitem realizar o cálculo do benefício.

Concentração

Este princípio defende a concentração dos bens a proteger em função da sua sensibilidade.

Tem como objectivo melhorar a eficiência da gestão das medidas de protecção, reduzindo as duplicações necessárias quando se tem de proteger diferentes repositórios de informação sensível com requisitos de protecção idênticos.

A observância deste princípio implica a classificação da informação quanto à sua sensibilidade, tópico esse que será detalhado em "Segurança da Informação", no capítulo "Áreas da Segurança Empresarial".

Protecção em Profundidade

A protecção em profundidade requer que os bens, e respectivas medidas de protecção, sejam dispostos de forma (física ou lógica) concêntrica, com os bens mais sensíveis no centro e os menos sensíveis no perímetro. Deste modo, a protecção é concebida sob a

forma de anéis concêntricos, que constituem barreiras sucessivas, gradualmente mais difíceis de transpor, à medida que o grau de sensibilidade da informação aumenta.

A aplicação deste princípio evita a existência de um conjunto de medidas de protecção distintas e avulsas, transformando-as numa sequência de obstáculos somados, adaptados aos fins a que se destinam. Na segurança física, por exemplo, as áreas contendo informação sensível não deverão, consequentemente, estar fisicamente expostas pela presença de portas e janelas com abertura directa para a rua.

Consistência

O princípio da consistência afirma que as medidas de protecção dos bens com grau de sensibilidade equivalente deverão ser, também, equivalentes, ou seja, a protecção deverá ser homogénea face à sensibilidade dos bens protegidos.

A sua aplicação implica um grau de protecção idêntico em todos os acessos, independentemente da sua natureza (o acesso físico ou o acesso lógico) ou grau de utilização, o que significa, por exemplo, que deverá ser evitada a situação clássica do porteiro e câmaras na porta da frente e apenas uma fechadura, destrancada, na porta das traseiras.

Redundância

O princípio da redundância dita a necessidade de empregar mais de uma forma de protecção para o mesmo fim, de modo a impedir que a protecção de um bem seja comprometida por uma única falha (ponto único de falha).

Exemplos típicos da sua aplicação são a utilização de *clusters*, de *firewalls* redundantes, ou a utilização de medidas de controlo de acesso físico distintas, tais como a presença de um porteiro junto a uma porta com fechadura.

São estes os princípios que o responsável pela segurança deverá dominar e articular na definição e implementação do Programa de Segurança. Quanto mais íntimo for o seu conhecimento das características, implicações e interacção entre eles, maior será a eficácia e melhores os resultados dos esforços desenvolvidos.

Modelos de Segurança

A segurança dos sistemas de informação é uma disciplina que nasceu com os técnicos que criaram esses sistemas e que, com a crescente utilização dos computadores e redes por todas as áreas empresariais, transitou para as mãos de gestores, ocupados com a implementação e gestão de um conjunto de medidas que se estende da esfera humana ao domínio tecnológico.

Ao longo dos anos, assistiu-se ao desenvolvimento e afirmação de um modelo de segurança, que hoje é omnipresente no tecido empresarial, designado “Fortaleza da Informação”. Esse modelo tem vindo, contudo, a revelar algumas fraquezas, devido à rápida evolução da tecnologia, pelo que se encontra já disponível uma alternativa para a sua sucessão.

Fortaleza da Informação

O modelo de protecção tradicional, que tem como ícone máximo a *firewall*, é frequentemente designado “Fortaleza de Informação”, numa analogia de carácter militar. Este modelo, baseado num monitor de referência, central, que aplica uma política de segurança, assenta em três princípios:

- política;
- integridade do monitor;
- secretismo.

Infelizmente nenhum destes princípios é sólido. As políticas deixam de ser geríveis quando o número de objectos e a complexidade das regras aumentam, como confirma a dificuldade registada na gestão mundana de algo tão simples como as palavras-passe (especialmente após o Verão). A integridade do sistema monitor de referência exige "apenas" a perfeição, uma vez que qualquer falha na muralha de protecção deixa entrar o inimigo, isto caso se consiga definir o perímetro[1], situação agravada pela dificuldade deste modelo em se degradar de forma graciosa: uma única falha é suficiente para comprometer toda a zona a defender. Por fim, o secretismo é extremamente difícil e dispendioso, sendo, regra geral, apenas viável quando aplicado a algumas chaves criptográficas.

Este modelo faz sentido num mundo em que o perímetro se encontrava perfeitamente definido, como no tempo dos computadores centralizados e monolíticos, que se distancia mais a cada nova funcionalidade introduzida pelas novas gerações de tecnologia. A fragilidade do "Modelo Fortaleza de Informação" é frequentemente apregoada numa frase que nos habituámos a ouvir: "a segurança é como uma corrente, tão forte quanto o seu elo mais fraco".

Cada vez mais, constatamos que a informação reside em sistemas sem segurança significativa (por exemplo, em PCs de secretária ou portáteis) e as "fortalezas" existentes vêem comprometida a sua estanquecidade (com, por exemplo, a abertura de portas VPN, ou pior, do ponto de vista da segurança, anexando aos sistemas pequenos "pacotes" de código produzidos por desconhecidos - *add-ins*, *snap-ins*, *applets*, etc.) Uma das consequências da utilização deste modelo é a perpetuação de soluções também desajustadas, que consistem frequentemente em "atirar tecnologia ao problema". Este acto serve o nosso sentimento de posse ("aquela caixa protege-nos"), mas não nos torna mais seguros.

---

[1] Segundo uma análise conjunta do CSI/FBI, realizada em 2002, a percentagem dos ataques registados em redes informáticas empresariais com origem no interior das mesmas situou-se nos 33%.

Os últimos anos assistiram à evolução das aplicações de negócio, que passaram de sistemas isolados (*stand-alone*) fechados, sobre os quais as organizações detinham total controlo, para sistemas abertos distribuídos, baseados em componentes *off-the-shelf* (COTS), dos quais as organizações têm um conhecimento e controlo limitados. Frequentemente, se não na quase totalidade dos casos, seleccionamos software segundo as funcionalidades oferecidas e o investimento inicial, em detrimento da sua robustez, maturidade e dos custos a longo prazo, ou indirectos.

Esta realidade retirou-nos a capacidade de resolução dos problemas de segurança de uma forma puramente tecnológica (o que era possível na "era do *mainframe*"), algo que é agravado pela visão redutora frequentemente encontrada nas administrações, que encaram as TI como custos, não envolvendo as áreas de negócio nos problemas encontrados e limitando-se ao pagamento da factura de segurança.

Sobrevivência da Informação

Face à grande dispersão do acesso aos dados, sistemas e código, aliada à elevada conectividade que o futuro parece ter reservada para nós, teremos de aceitar a visão e controlo limitados que temos sobre a parte da "imagem global" sob a nossa alçada. A este factor juntam-se as necessidades de protecção, e já não só das tecnologias de suporte aos objectivos da organização, num contexto hostil em que é cada vez mais difícil isolar perímetros ou áreas em que se possa confiar.

Para satisfação das necessidades supracitadas, surgiu um novo modelo, designado "Modelo de Sobrevivência da Informação", que integra o conceito da sobrevivência com o da gestão do risco pelo negócio[2], obrigando à utilização de estratégias de gestão do risco baseadas num conhecimento íntimo da missão a proteger.

---

[2] Nesta abordagem é o negócio que aceita, transfere ou controla os riscos.

Este modelo tem como princípios:

- envolvimento;
- exposição;
- emergência;
- diversidade;
- contexto.

O primeiro destes princípios, o envolvimento, torna a segurança num problema de toda a organização, pelo que a viabilização de algumas soluções só pode ser avaliada no contexto do negócio, permitindo transcender soluções puramente técnicas (por exemplo, recorrendo a advogados para introduzir cláusulas de [des]responsabilização nos contratos).

A exposição nega a qualquer componente imunidade a ataques, acidentes ou falhas, ou seja, segundo este princípio não existem santuários.

O terceiro princípio afirma que as propriedades globais de sobrevivência surgem (emergem) da combinação de componentes que isoladamente não são sobreviventes.

A diversidade, de há longa data a melhor amiga da segurança, introduz o bom senso de “não colocar os ovos todos no mesmo cesto”.

Por fim, o contexto refere que as soluções técnicas deverão ser baseadas no verdadeiro ambiente em que os sistemas operam e não nas funcionalidades disponíveis no sistema, ou na forma correcta de os usar. É um assentar dos pés na terra para os informáticos.

A implementação deste modelo assenta na análise da capacidade de sobrevivência dos sistemas e na posterior identificação de estratégias de mitigação de riscos, através da promoção das capacidades de resistência, reconhecimento e recuperação de falhas, aumentando a segurança dos sistemas de informação.

Identificado o modelo considerado adequado para a segurança da Empresa, será agora necessário analisar um outro modelo, o de maturidade, que permite identificar o caminho a percorrer.

Modelo de Maturidade

O Programa de Segurança de uma empresa passa por vários estádios de desenvolvimento, cuja ultrapassagem representa amadurecimento. Esses graus de maturidade correspondem à:

1) definição de políticas e normas de segurança;
2) definição da arquitectura e dos processos da segurança;
3) implementação dos processos de suporte à inspecção, protecção, detecção e reacção;
4) realização de acções de sensibilização e de formação em segurança;
5) realização periódica de auditorias e testes à segurança;
6) implementação de processos de resposta reflexa;
7) validação do modelo de protecção e da sua implementação.

Para que a maturidade de segurança esteja num determinado grau, segundo este modelo, é necessário que a Empresa complete o grau em causa e todos os graus anteriores a esse. Por exemplo, para atingir o grau 3 no modelo de maturidade, será necessário primeiro cumprir razoavelmente os requisitos dos graus 1 e 2. Apesar da subjectividade associada à implementação de cada grau, este modelo será a medida mais realista disponível para determinar a maturidade do Programa de Segurança.

A situação registada numa empresa em matéria de segurança, regra geral, corresponde ao preenchimento parcial, em simultâneo, de diversos graus, o que não é, por si só, preocupante. Tal facto reflecte apenas alguma preocupação desconexa com a segurança, que terá sido implementada de forma não orientada, tipicamente

sem o fio condutor conferido por uma política e um plano global de segurança.

Ao definir o Plano Global de Segurança, que será abordado em "Criação do Plano de Segurança", o responsável por esta área deverá procurar preencher cada grau de maturidade do modelo dentro das limitações presentes, antes de introduzir medidas correspondentes aos níveis de maturidade superiores.

A segurança é um processo complexo, com componentes tecnológicas e humanas, envolvendo metodologias e comportamentos. Para permitir a implementação dos modelos desejados, necessitamos conhecer os aspectos humanos da organização, sendo necessário traçar o perfil, na medida do possível, dos intervenientes directos e indirectos na segurança da Empresa, ou seja, dos actores da segurança, analisando os seus papéis, comportamentos e motivações.

Os Actores da Segurança

Os actores da segurança são infinitos, pelo menos potencialmente. De elementos internos à Empresa a perfeitos estranhos, de clientes a parceiros, passando obviamente pelos funcionários, todos podem ter um impacto positivo ou negativo sobre a segurança da mesma.

Em seguida irão considerar-se os personagens mais comuns e identificar a forma como podem ser auxiliados a cumprir os seus papéis na segurança da Empresa.

Administração da Empresa

A Administração, bem como os agentes por esta nomeados, são os proprietários da informação usada pela Empresa na sua relação com os clientes e na produção e comercialização dos seus bens. É ela quem decide o que irá ser feito, o que invariavelmente tem repercussões na segurança, uma vez que esta se encontra depen-

dente tanto das suas decisões nesta matéria, como do comportamento, mais ou menos seguro, dos utilizadores.

Por outro lado, este órgão é ainda responsável perante o Governo e outras instituições nacionais e internacionais pelo cumprimento de leis e demais disposições, o que pode ser lido como, entre outros, um factor de responsabilidade no que diz respeito à segurança interna e externa da organização.

Para o Negócio, a segurança afigura-se paradoxalmente como um custo e uma necessidade para a sua sobrevivência. Se, por um lado, fazer um produto ou Empresa com maior segurança raramente é visto como uma mais-valia significativa, por outro, o perigo de um desastre não é ignorado de todo, sendo, para os corpos gerentes, uma questão de efectuar investimentos em medidas de prevenção e protecção para evitar potenciais perdas.

Perante a sociedade, e em matéria de segurança, a Administração tem a necessidade de mostrar "*due diligence*", ou seja, de mostrar que fizeram o que é considerado razoável pelo senso comum e no cumprimento da legalidade.

Naturalmente, a principal motivação da Administração é para com a satisfação dos accionistas e, como tal, dos clientes, implicando frequentemente um elevado grau de disponibilização de informação, o que poderá não ser facilmente compatibilizado com uma boa segurança. O papel do responsável pela segurança na Empresa, junto deste órgão, é mostrar as principais alternativas presentes e as suas implicações, facultando-lhe a informação que esta necessita para tomar decisões informadas, contribuindo, desse modo, para a melhoria do nível de segurança.

Utilizadores

Utilizadores são todos aqueles que usam os sistemas de informação, independentemente dos privilégios que detenham. Os conhecimentos técnicos do utilizador típico variam muito, dependendo tanto da actividade desenvolvida como da faixa etária predomi-

nante, sendo os níveis médios mais elevados em empresas tecnológicas ou em que os colaboradores se encontrem predominantemente numa faixa etária mais jovem.

Os utilizadores são quem executa as actividades (tecnológicas ou não) de suporte aos processos do negócio. Do ponto de vista da segurança, fazem toda a diferença, podendo ser um elo fraco, ou, pelo contrário, um catalisador que fortalece a cadeia, sendo uma peça essencial no processo da segurança.

Em qualquer grupo de utilizadores de dimensão significativa irá encontrar-se sempre uma percentagem mais ou menos reduzida de tecnofóbicos e de "curiosos". Enquanto que os primeiros raramente representam uma ameaça significativa (excepto para o seu desempenho, naturalmente) os últimos são frequentemente um problema. Os "curiosos" são indivíduos com uma forte motivação para efectuar tarefas de elevada complexidade técnica, sem que possuam os conhecimentos necessários à correcta execução das mesmas. O resultado é que frequentemente são apanhados pelas consequências das suas acções, que, regra geral, afectam os que os rodeiam. Um sub-grupo particularmente perigoso dos "curiosos" é o dos designados "*script-kiddies*", que são indivíduos que consideram a noção de *hacker* romântica, sonhando com feitos fantásticos e mediáticos. Infelizmente, os *script-kiddies* são famosos por experimentarem receitas de *hacking* disponíveis na Internet sem terem noção das implicações reais das mesmas, receitas essas passíveis de causar tantos danos como um ataque verdadeiramente sofisticado.

A principal característica comportamental dos utilizadores é a sua tendência para facilitarem os processos que executam: se existirem duas maneiras de fazer a mesma coisa (por exemplo, memorizar uma palavra passe complexa ou escrevê-la num papel que se cola por baixo do teclado), um utilizador que não esteja especialmente sensibilizado para esse efeito irá invariavelmente adoptar o comportamento mais cómodo (e deixar a palavra passe acessível), derrotando inconscientemente a segurança em prol do menor esforço.

É pois necessário, numa aplicação directa da "Lei" de Murphy[3], definir as medidas de prevenção, partindo do princípio que se os sistemas de informação tiverem uma vulnerabilidade, esta acabará por ser explorada pelo utilizador.

A principal forma de ajudar os utilizadores a adoptar a segurança é a sua sensibilização, tanto por campanhas de divulgação, como através de sessões de esclarecimento e formação, mostrando-lhes as razões do que lhes é solicitado e a forma segura de realizar as suas actividades quotidianas como, por exemplo, através da aplicação da política de secretária limpa e da destruição sistemática, em equipamento adequado, dos documentos sensíveis, em vez de os deitar simplesmente no lixo. Em matéria de sensibilização dos utilizadores deverá observar-se sempre o princípio "*Keep It Short and Simple*"[4], ou KISS, que nos diz que devemos simplificar a linguagem utilizada, particularmente no que diz respeito à linguagem técnica, devido à disparidade do nível de conhecimentos existente no universo de utilizadores.

Informáticos

Os equipamentos, software e outros recursos (redes, aplicações, etc.) necessitam de gestão diária, recaindo essa atribuição sobre indivíduos cuja designação varia consoante a tecnologia em causa (por exemplo, *root*, administrador) e o âmbito dos seus poderes (administrador de utilizadores, de impressoras, de armazenamento, de antivírus, etc.). Independentemente da sua designação, estes "utilizadores especiais" são, regra geral, conhecedores das implicações das suas acções sobre os sistemas que gerem, embora possam desconhecer em detalhe as vulnerabilidades particulares desses sistemas.

---

[3] "Tudo o que pode correr mal, irá correr mal."

[4] "Manter tudo curto e simples".

Os colaboradores da empresa envolvidos de alguma forma na gestão dos sistemas de informação são apelidados, comummente, de "*informáticos*". Neste grupo, existem desde os meros curiosos, aos técnicos e administradores. Atendendo a que os conhecimentos dos curiosos pouco ultrapassam os dos utilizadores médios, vamos debruçar-nos sobre os dois últimos.

A principal distinção entre técnico e administrador prende-se com a centralização dos sistemas. Os técnicos são os elementos responsáveis por actos de gestão de sistemas com impacto exclusivamente local, enquanto que os administradores gerem os sistemas centrais. Esta definição é algo precária, no entanto, face à centralização/descentralização cíclica que afecta regularmente os sistemas de informação.

Ao nível da implementação, os administradores informáticos desempenham o papel mais importante na segurança, abaixo do nível estratégico/decisório, uma vez que as medidas que implementam atingem uma população alargada. Por outro lado, os técnicos, ao implementarem em massa acções junto dos utilizadores (por exemplo, instalando o sistema operativo nas estações de trabalho) replicam por um número significativo de sistemas quaisquer vulnerabilidades que possam existir.

Na realidade, a designação "informático" descreve mais uma forma de pensar, e o comportamento associado, do que uma função. Uma graça que ilustra esta forma de pensar é o ditado "99% dos problemas de um sistema encontram-se entre o teclado e a cadeira", o que indicia incompreensão dos aspectos humanos e da componente de inteligência emocional existente nos processos que assentam na tecnologia por eles suportada. Por sua vez, a esta incompreensão encontra-se associada uma postura tecnológica (quase evangelizadora) na resolução dos problemas, que se expressa na promoção recorrente de soluções tecnológicas, em detrimento de outros tipos (por exemplo, a alteração do procedimento) que podem inclusivamente ser preferíveis, tanto do ponto de vista da segurança, como economicamente.

Uma regra elementar de promoção da segurança, relativamente aos técnicos, é a da atribuição de privilégios segundo o princípio do menor privilégio, que dita que não deverá ser permitida a realização de acções que não sejam necessárias ao desempenho da actividade (por exemplo, se é suposto um técnico gerir impressoras numa rede Microsoft, ele não deverá poder também adicionar computadores ou utilizadores ao domínio). Esta preocupação deverá ainda ser complementada com a configuração dos sistemas, por forma a gerar um rasto de auditoria, algo que iremos abordar mais adiante no capítulo "Áreas da Segurança Empresarial".

Uma vez que a Administração dos sistemas de informação é uma função para a qual é necessário um elevado nível de confiança, a principal forma de promover a segurança junto destes actores é através da definição de políticas, normas e procedimentos de operação segura, bem como pela promoção de acções de formação sobre os aspectos técnicos (da segurança) dos sistemas que administram.

Clientes

Os clientes são, de certa forma, quem nos paga os ordenados. São eles os "patrões dos patrões", ou seja, quem dita o que necessitamos fazer como Empresa.

O cliente típico não quer saber o que está por trás do produto ou serviço que adquire, assumindo que é tão seguro quanto o valor que reconhece à marca. Este capital de confiança que a Empresa detém junto do cliente é volátil e pode desaparecer, bastando para tal algo tão simples como a atenção inusitada dos media, sendo então difícil recuperá-lo.

À semelhança dos utilizadores, os clientes contornarão a segurança em prol da comodidade, se lhes for dada oportunidade para tal, algo que é potenciado pela inexistência de um vínculo forte à Empresa. Desta forma, dificilmente se poderá contar com eles para promover a segurança.

Apesar disso, a Empresa pode impor-lhes regras na utilização dos seus produtos e serviços. Estas regras devem, no entanto, ser claramente justificáveis, de forma compreensível para o cliente. Outra forma de reduzir o risco na interacção com os clientes é a introdução de formas de monitorização, nos casos em que não for possível introduzir uma utilização segura.

Parceiros

Os parceiros da Empresa são as entidades externas que participam de múltiplas formas nos processos de negócio, tanto ao nível dos canais de distribuição, como na produção.

Estes actores podem assumir uma parte, ou mesmo a totalidade, dos processos de segurança da Empresa, ou constituir apenas uma componente dos processos de negócio.

Regra geral, os parceiros não têm interesse na nossa segurança, desde que esta, ou a sua ausência, não os afecte negativamente. Porém, casos há em que a segurança pode constituir um pré-requisito para a parceria.

Os parceiros, normalmente são escolhidos ao nível estratégico pela Administração, devem ser avaliados também pela sua postura de segurança, através, por exemplo, da análise das suas políticas e planos de recuperação. Nos casos em que tal não é possível, e apenas nesses casos, será necessário recorrer à contratualização explícita dos aspectos relacionados com a segurança, como forma alternativa de promover a segurança da Empresa junto dos parceiros. Nas situações em que a segurança é contratualizada, deve-se ter especial cuidado para não se incorrer numa confiança cega no Parceiro, sendo necessário, por exemplo, verificar se o fornecedor do serviço de recuperação de desastre de que dependemos para sobreviver poderá ser afectado pelo mesmo desastre, pois nesse caso, por melhor contratualizado que o serviço estiver, não teremos garantias do seu fornecimento.

Pessoal Temporário

O pessoal temporário é similar aos restantes utilizadores da empresa, no seu comportamento, embora a sua ligação à Empresa seja mais ténue, o que requer a introdução de medidas que impeçam a extensão dos privilégios de acesso aos sistemas de informação para além do fim do vínculo à Empresa, e em particular, de uma eficiente metodologia de gestão de contas e privilégios face à saída da empresa.

Outro aspecto importante diz respeito à adaptação dos processos de sensibilização para a segurança à duração do ciclo de vida do vínculo, o que pode ser acautelado, por exemplo, através de formação inicial e da assinatura de um acordo de confidencialidade e de aceitação da política de segurança da Empresa.

Conclusão

Este capítulo apresentou, de forma resumida, os elementos que o responsável pela segurança deverá equacionar no desempenho da sua função.

Face à diversidade da composição das empresas e à sua mutação com o passar do tempo, existirão, naturalmente, muitas variações ao que foi exposto, pelo que uma boa dose de flexibilidade e mesmo de capacidade de improvisação é altamente recomendável. A realidade raramente espelha a teoria e a miríade de situações possíveis é quase infinita. Assim, ao seleccionar um modelo de segurança e ao interagir com os vários actores, o responsável pela segurança deverá, sempre, contar com a possibilidade de desvios ao plano.

No próximo capítulo iremos abordar um conjunto de metodologias que permitirão identificar as áreas de intervenção sobre as quais as medidas de segurança deverão incidir, bem como o equilíbrio dessas medidas com o respectivo impacto sobre a organização.

Capítulo II - Gestão do Risco

A gestão do risco é o processo de identificação de um conjunto de medidas que permitam conferir à Empresa o nível de segurança pretendido pela sua Administração.

Este processo faz parte integrante do Programa de Segurança da Empresa e é composto por uma sequência de fases, em que os riscos são determinados e classificados, sendo depois especificado um conjunto equilibrado de medidas de segurança (designadas por controlos) que permitirão reduzir ou eliminar os riscos a que a Empresa se encontra sujeita.

As etapas do processo de gestão do risco são:

1. Identificação dos riscos;
2. Análise de risco;
3. Identificação de controlos;
4. Selecção de controlos.

Neste capítulo serão analisadas estas diversas fases, com excepção da identificação de controlos, uma vasta área abordada mais adiante neste livro.

Em seguida será detalhada a primeira fase da gestão do risco, sendo identificado o contexto da Empresa em termos de risco.

Identificação dos Riscos

A gestão do risco inicia-se com a sua identificação, que é conseguida através do levantamento do contexto de risco em que a Empresa existe e actua.

Para contextualizar a Empresa poderão ser empregues diversos modelos:

SWOT: (*strengths, weaknesses, opportunities and threats*[5]) definição da relação entre a Empresa e o ambiente através da identificação dos pontos fortes, fracos, oportunidades e ameaças à sua segurança.

Contexto: descrição da Empresa, das suas capacidades, metas, objectivos e estratégias implementadas para os alcançar.

Alvo: descrição das metas e objectivos, estratégias, âmbito e parâmetros da gestão do risco.

Bens: descrição dos bens da Empresa e das suas interdependências.

Uma vez contextualizado o cenário de risco em que a Empresa está presente, poderá iniciar-se a identificação dos elementos necessários à análise de risco: as ameaças e vulnerabilidades existentes e os bens que poderão estar em perigo.

Um ponto importante a reter, ao realizar qualquer levantamento, é o facto do levantamento e posterior análise de risco não constituírem um fim por si só, uma vez que o objectivo do levantamento é permitir a análise e o da análise é permitir a implementação consistente das medidas de protecção. É, então, por isso que todo o processo não deverá consumir uma quantidade inusitada de recursos, o que requer alguma reflexão e espírito prático na escolha do método de análise (qualitativa ou quantitativa), que deverá ter em conta o esforço requerido para a recolha da informação necessária. Apesar de teoricamente ser preferível realizar uma análise quantitativa, os recursos que esta requer poderão não ser justificados, sendo preferível optar pela realização de uma análise qualitativa. Em qualquer caso, o processo de recolha preliminar de informação e posterior análise não deverão nunca levar mais de alguns dias, uma vez que

[5] Pontos fortes, pontos fracos, oportunidades e ameaças.

num universo empresarial em constante mutação, uma análise com demasiado detalhe ficará rapidamente desactualizada.

Ameaças

As ameaças[6] à Empresa podem ser identificadas tanto através da produção de cenários como pela criação de listas de tipificação. A listagem das ameaças por tipo facilita a obtenção de informação estatística sobre a sua frequência de ocorrência no passado, informação essa que é importante para o passo posterior de análise dos riscos colocados por estas ameaças.

A forma clássica de tipificação dos riscos consiste na definição de categorias e subcategorias de classificação, criando-se uma "árvore", em que os ramos correspondem aos tipos de ameaça e as folhas às ameaças em si. Nesta forma de classificação, algumas das categorias principais mais comuns são as apresentadas na Fig. II-1.

Uma vez completa, a árvore de ameaças da Empresa poderá chegar a ter mais de um milhar de ramos/folhas, embora a sua dimensão e composição dependa, naturalmente, de muitos factores, tais como a área de actividade (serviços, indústria, etc.), dispersão geográfica, dimensão, tipo de actividade, etc.

---

[6] Para a correcta compreensão deste capítulo é recomendada a consulta dos conceitos RISCO, AMEAÇA, VULNERABILIDADE e IMPACTO na lista de terminologia apresentada no final do livro.

Árvore de Ameaças

Desastres ou perigos:

- de causa natural
  - provocados por água
    - cheias
    - inundações
    - …
  - provocados por fogo
    - incêndios florestais
    - ...
  - provocados por fenómenos sísmicos
  - provocados por vento
    - tempestades
  - provocados por electricidade
    - relâmpagos
    - descargas de energia
  - provocados por agentes biológicos ou virais
    - epidemias
  - desabamentos
- com origem humana
  - acidental
    - fogo
    - inundações
    - derrames de substâncias químicas ou biológicas
    - explosões
    - queda/despiste de veículos (carros, comboios, aviões, barcos, etc.)
    - introdução incorrecta de dados nos sistemas
    - configuração incorrecta dos sistemas
  - intencional
    - quebras contratuais
    - terrorismo
    - tumultos
    - greves
    - furto
    - fraude
    - sabotagem
- ...

Fig. II-1: Árvore de ameaças - Exemplo

Para criar esta árvore, o responsável pela segurança da Empresa poderá utilizar como ponto de partida as muitas listas de ameaças existentes na Internet e na literatura, que servirão de base para a

realização de entrevistas que permitirão colmatar a informação requerida ao processo de definição da lista final.

Vulnerabilidades

A identificação das vulnerabilidades visa permitir aproximar o cálculo da probabilidade de concretização das ameaças inerentes à realidade da Empresa.

Exemplo: qualquer empresa está sujeita ao terrorismo, embora uma organização ligada a uma facção num conflito "quente" tenha de encarar este risco como real.

À semelhança do que se verifica no processo de levantamento das ameaças, a identificação das vulnerabilidades pode ser suportada pela criação de uma árvore tipológica, cujas folhas serão, naturalmente, vulnerabilidades em vez de ameaças (ver Fig. II-2).

Árvore de Vulnerabilidades

Origem:

- localização/dispersão geográfica
  - das instalações
    - instalações em locais inacessíveis a meios de socorro
    - instalações em locais densamente povoados
- política
  - postura política do país da Sede
- ...

Fig. II-2: Árvore de vulnerabilidades - Exemplo

Por fim, relativamente à identificação das vulnerabilidades da Empresa, convém referir que o trabalho realizado nesta matéria deverá ser sempre classificado de Confidencial (ou equivalente), dada a sua natureza particularmente sensível.

Bens

A identificação dos bens é necessária apenas na análise quantitativa do risco, em que o risco é medido pelo impacto resultante da concretização da ameaça.

A principal dificuldade na identificação dos bens, bem como na estimativa dos danos, regista-se relativamente aos bens intangíveis, uma vez que o seu carácter subjectivo dificulta a definição de modelos e métricas.

Exemplo: a ameaça de quebra de confidencialidade pela divulgação acidental de informação (por exemplo, da árvore de vulnerabilidades da Empresa) pode gerar perdas intangíveis na imagem da marca e até mesmo na preferência demonstrada pelos clientes. Neste caso particular, em que a identificação dos bens até é relativamente óbvia, será difícil quantificar as perdas, ou seja, estimar o decréscimo de vendas.

Uma forma de facilitar a quantificação do valor dos bens é a definição e utilização de escalões, permitindo usar aproximações para evitar cálculos complexos (ver exemplo da Fig. II-3).

Categorias de valor

Escalão	Intervalo
0	até € 500
1	€ 501 a € 5.000
2	€ 5.001 a € 50.000
3	mais de € 50.000

Fig. II-3: Categorias de valor dos bens - Exemplo

Análises de Risco e de Impacto

A análise de risco é o processo que permite usar a informação existente de forma sistemática, para determinar o grau de exposição da Empresa aos diversos tipos de acontecimentos perigosos a que se encontra sujeita. Após a identificação das ameaças, vulnerabilidades e bens, apresentada anteriormente, a análise de risco irá ocupar-se da caracterização dos riscos, pela quantificação ou qualificação da probabilidade das ameaças gerarem danos ou, alternativamente, dos danos decorrentes da concretização das diversas ameaças expectáveis.

Esta análise constitui a base do processo de selecção e recomendação das medidas identificadas para redução das vulnerabilidades (ver "Estratégia de Controlo" mais adiante neste capítulo).

O outro tipo de análise aqui apresentado será a de impacto no negócio, através da qual são determinadas as actividades críticas para a sobrevivência da Empresa em caso de desastre, servindo, também, esta análise como base ao processo de criação do plano de continuidade do negócio (ver "Segurança Face ao Desastre").

Análise de Risco Quantitativa

A Exposição Anual à Perda (ou *Anual Loss Exposure* – ALE) é uma metodologia de análise de risco quantitativa, que permite estimar o risco através do cálculo do valor da perda expectável decorrente de uma determinada ameaça.

Esta análise de risco assenta nas duas fórmulas seguintes:

$$ALE = Valor \times R$$

$$R = V \times P$$

Onde: *ALE*: perda monetária média expectável num ano, expressa numa unidade monetária.

Valor: valor acumulado dos danos provocados pela concretização da ameaça (expresso numa unidade monetária).

R: probabilidade de concretização da ameaça na Empresa no período de um ano (expresso em ocorrências por ano).

V: número que representa a vulnerabilidade da Empresa à ameaça (sem unidade).

Exemplo:	V = 0	Empresa invulnerável à ameaça.
	V = 1	Empresa com exposição normal à ameaça.
	V > 1	Empresa com uma exposição à ameaça superior à registada na média do universo do estudo para o cálculo da probabilidade (P).

P: probabilidade correspondente ao número médio esperado de vezes que a ameaça se irá concretizar por ano (expresso em ocorrências por ano).

Exemplo:	P = 1	A ameaça concretiza-se uma vez por ano.
	P = 0,1	a ameaça concretiza-se uma vez por década.
	P = 12	a ameaça concretiza-se uma vez por mês.

Exemplo: considerando uma empresa com um *datacenter* avaliado em € 300.000, situado por baixo de uma cantina, num edifício equipado com sistemas de extinção por água, qual é ALE do risco de perda do equipamento do *datacenter* devido a um incêndio?

Considerando que em média poderá ocorrer um incêndio grave a cada cem anos, que o tipo de mecanismo de extinção provocará a destruição dos equipamentos em caso de activação e que a presença da cantina aumenta em 50% o risco de incêndio:

$P = 1/100 = 0,01$

$V = 1,0$ (normal) + 0,5 (da cantina) + 0,2 (do sistema de extinção)

$R = 0,01 \times 2,0 = 0,02$

$ALE = 300.000 \times 0,02 = 6,000$

Segundo esta metodologia, o risco de perda do equipamento em causa corresponde a uma exposição da ordem dos seis mil Euros por ano, podendo-se então justificar a introdução de controlos com um custo anual abaixo deste valor.

Um problema que não é considerado directamente nesta metodologia é que a distribuição das perdas, em caso de desastre, não é proporcional, ou seja, tanto um acidente no primeiro ano como ao fim de cem anos causam a totalidade dos danos, pelo que poderá ser necessária a utilização de métodos mais elaborados, com recurso a distribuições estatísticas complexas (como, por exemplo, a distribuição de Poisson), que não serão discutidos aqui.

Análise de Risco Qualitativa

A metodologia que se irá abordar visa evitar o perigo de inacção decorrente de um esforço excessivo de análise, fenómeno também

designado por "*paralysis by analysis*" (paralisia pela análise). Para tal, a prioritização dos riscos é efectuada de forma subjectiva, estando, naturalmente, a qualidade dos resultados dependente dos conhecimentos e capacidade da equipa que realiza a análise e da objectividade de quem a coordena.

A análise de risco qualitativa assenta nas seguintes quatro fases:

1. Constituição da equipa;
2. Realização de sessões de classificação das ameaças;
3. Realização de sessões de classificação dos impactos; e
4. Cálculo dos riscos.

A composição da equipa desempenha um papel preponderante no seu resultado final, pelo que o responsável pela segurança da Empresa deverá evitar a tentação de a realizar sozinho, ou apenas com os membros da sua equipa, e reunir um grupo com elementos competentes que representem diversas áreas, integrando:

- proprietários das aplicações/informação;
- administradores de sistemas/aplicações/bases de dados, etc.;
- especialistas nas diversas áreas tecnológicas;
- utilizadores;
- programadores;
- analistas;
- gestores de produção e operação;
- representante do departamento jurídico; e, se necessário,
- consultores.

Adicionalmente, a representatividade conferida por uma lista abrangente de participantes irá garantir que os controlos recomendados na sequência da análise de risco produzida serão bem aceites pelas áreas afectadas.

Após a constituição da equipa de análise de risco qualitativa, serão organizadas sessões para discussão e posterior preenchimento da ficha de classificação das ameaças (ver exemplo da Fig. II-4), através da atribuição de valores para o grau de probabilidade e de impacto de cada uma delas. Esta classificação poderá ser efectuada quer por consenso, quer pela média das classificações individuais atribuídas pelos diversos membros.

Ameaça	Probabilidade	Impacto	Risco
Incêndio	1	5	
Inundação	2	1	
Furto	2	2	
...	...	...	

Fig. II-4: Ficha de classificação das ameaças - Exemplo

Nestas sessões, o papel do coordenador da análise é preponderante, pelo que este elemento deverá observar o seguinte conjunto de regras para facilitar o processo e garantir a sua concretização:

- fomentar a participação;
- não preleccionar;
- manter a discussão dentro do tópico agendado (classificação de uma ameaça específica) e da duração predefinida;
- manter a neutralidade e evitar animosidade;
- ouvir mais e falar menos; e
- garantir o registo de todas as contribuições.

Uma vez que o processo de classificação irá fazer sobressair as divergências de ponto de vista dos participantes, quer devido a traços particulares de personalidade ou aos seus contextos profissio-

nais distintos (informáticos, administrativos, juristas, etc.), será necessário adoptar algumas regras para evitar perdas de tempo e até mesmo potenciais conflitos. Desta forma, o coordenador deverá especificar um conjunto de regras para a realização das sessões de classificação das ameaças e dos impactos, que poderão incluir:

- todos participam – não há exclusões;
- não sair do tópico;
- todas as ideias são igualmente válidas;
- só se debate um tema de cada vez;
- cada ponto é discutido num tempo predefinido; e, por fim,
- os participantes deverão ser sucintos, justos e correctos.

Após a conclusão dos processos de classificação, o risco será calculado através de uma relação simples entre a probabilidade e o impacto apurados.

Exemplo: a fórmula

$$\text{Risco} = \text{Probabilidade} + \text{Impacto}$$

representa uma relação possível para o cálculo do risco, que permite uma abordagem equilibrada entre a frequência de concretização da ameaça e o seu impacto.

Análise de Impacto no Negócio

Michael E. Porter, um reputado professor da Universidade de Harvard, estabeleceu uma cadeia organizacional, cuja gestão condiciona a vantagem competitiva das empresas. Nessa cadeia, conhecida por Cadeia de Valor de Porter, as funções de negócio assentam em processos (actividades primárias) que, por sua vez, são sustentadas por actividades de suporte (ver Fig. II-5).

A análise de impacto no negócio visa apurar quais as funções, processos e actividades de suporte (tecnológicas ou não) críticas para o funcionamento da Empresa.

Uma vez que, para qualquer colaborador da Empresa, as tarefas por si desempenhadas são essenciais (em detrimento das restantes), a identificação do que é realmente crítico deverá seguir uma abordagem *top-down*, ou seja, de uma visão mais estratégica até à operacional. Assim, deverá começar-se por identificar as funções críticas do negócio, identificando seguidamente, de entre os processos que o compõem, aqueles que são essenciais e, finalmente, quais das actividades de suporte a estes processos são igualmente vitais para a realização do processo em questão.

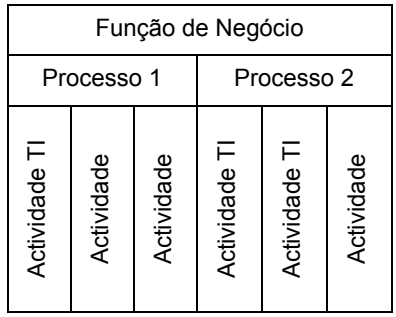


Fig. II-5: Funções de Negócio, Processos e Actividades de Suporte

Seguindo esta abordagem, será garantido o funcionamento de todas as funções críticas, sem o ónus da identificação de processos ou de actividades de suporte que não contribuem para a viabilidade da Empresa em caso de desastre.

Porém, não existem funções, processos ou actividades não críticos, uma vez que a sua própria existência denota a necessidade do seu funcionamento por parte da Empresa. O que se verifica é que cada um contribui de forma maior ou menor para o seu correcto funcionamento e que algumas acabam por afectar a própria viabilidade da

organização caso estejam indisponíveis durante um determinado período, que poderá ser mais breve ou mais longo. Ao classificar uma função como "crítica" estaremos, na realidade, a indicar que a tolerância da Empresa à sua indisponibilidade (ou à sua disponibilidade sem informação completa e actualizada) é menor que o tempo necessário à recuperação dessa função sem recurso a mecanismos de protecção contra desastre.

Desta forma, a análise de impacto de negócio deverá determinar simultaneamente o período de indisponibilidade tolerada e o impacto resultante de uma indisponibilidade para além desse prazo. A cada prazo de indisponibilidade tolerada e de impacto associado deverá fazer-se equivaler um tempo alvo de recuperação (TAR), que poderá ser ajustado posteriormente durante o processo de identificação de dependências.

Consideremos os tempos alvo de recuperação indicados no exemplo da Fig. II-6, recolhidos numa análise fictícia de impacto no negócio, em que cada função, processo ou actividade é caracterizado por um TAR próprio, que representa o período durante o qual esse elemento pode estar indisponível sem gerar, por si só, um impacto negativo desastroso.

Apesar dessa análise determinar o tempo alvo para a recuperação de cada processo e actividade que suporta a função do negócio, esses valores não entram em linha de conta com as interdependências existentes. Para tal, será necessário determinar o menor TAR registado em todas as ocorrências (da actividade ou processo) e aplicar esse valor a todas. Seguidamente deverá proceder-se aos ajustes dos restantes TAR afectados pelas substituições, encontrando-se desta forma os objectivos de recuperação efectivos para toda a Empresa.

Crítico: TAR < 15 dias

Função	Vendas **Crítica** TAR = 3 dias						
Processos	Facturação **Crítico** TAR = 7 dias			Logística **Crítico** TAR = 1 dia		Promoção de produtos **Não crítico** TAR = 60 dias	
Actividades	Emissão **Crítica** TAR = 7 dias	Balanço **Não crítica** TAR = 1 mês	Cobrança **Crítica** TAR = 3 dias	Emissão **Não crítica** TAR = 1 mês	Expedição **Crítica** TAR = 2 h	Linha azul N/A	CRM N/A

N/A: não apurado

Fig. II-6: Tempos Alvo de Recuperação - Exemplo

Exemplo: atendendo às dependências existentes entre a função, os processos e as actividades do exemplo da Fig. II-6, o TAR a implementar para a actividade "Emissão" deverá ser ajustado de modo a garantir a recuperação da função de negócio em tempo útil. Após consideração das interdependências existentes, serão definidos os seguintes objectivos:

1. Actividades com requisito de recuperação inferior a um dia:
   - Expedição
2. Actividades com requisito de recuperação entre um dia e uma semana:
   - Emissão

- Cobrança

3. Actividades com requisito de recuperação entre uma e duas semanas:

   - Nenhuma

   As restantes actividades do exemplo não são consideradas críticas, uma vez que os seus TAR se encontram para além do limite definido de 15 dias.

A análise de impacto permitiria, neste caso, ordenar as actividades críticas, dando prioridade à escolha das medidas de controlo a adoptar.

Estratégia de Controlo

Uma vez conhecida a situação da Empresa em termos de riscos, é chegado o momento de definir as medidas que deverão ser postas em prática para aumentar a sua segurança. O passo seguinte à análise de risco é a identificação e selecção dos controlos, ou seja, dos processos ou dispositivos que permitam reduzir o efeito da ameaça ou os danos decorrentes da sua concretização.

A gestão estratégica da segurança da Empresa implica uma atenção muito particular ao processo de selecção dos controlos, que deverá garantir uma abordagem consistente e abrangente, assente nos princípios da segurança já apresentados (ver “Princípios de Prevenção e Protecção” no capítulo “Teoria da Segurança”).

Arquitectura

Muito raramente a definição dos sistemas de informação da Empresa é feita tendo por base uma estratégia global para a sua segurança. Na vasta maioria dos casos, o responsável pela segurança é contratado quando os sistemas já se encontram em produção, pelo que as oportunidades de revolução são bem menores do

que as de evolução. A introdução de controlos será, provavelmente, realizada em intervenções mais ou menos pontuais, correndo-se o risco de perda de consistência através da introdução de controlos desconexos e não abrangentes. Para lidar com este problema, a equipa de segurança deverá, juntamente com especialistas internos e externos à Empresa, definir um plano de construção da infra-estrutura da segurança, ou seja, definir a arquitectura alvo para a segurança dos sistemas de informação.

A definição da arquitectura deverá começar pela identificação de um objectivo de alto nível, como o apresentado na Fig. II-7, que poderá ser detalhado progressivamente em antecipação à introdução de cada controlo.

Arquitectura de Segurança

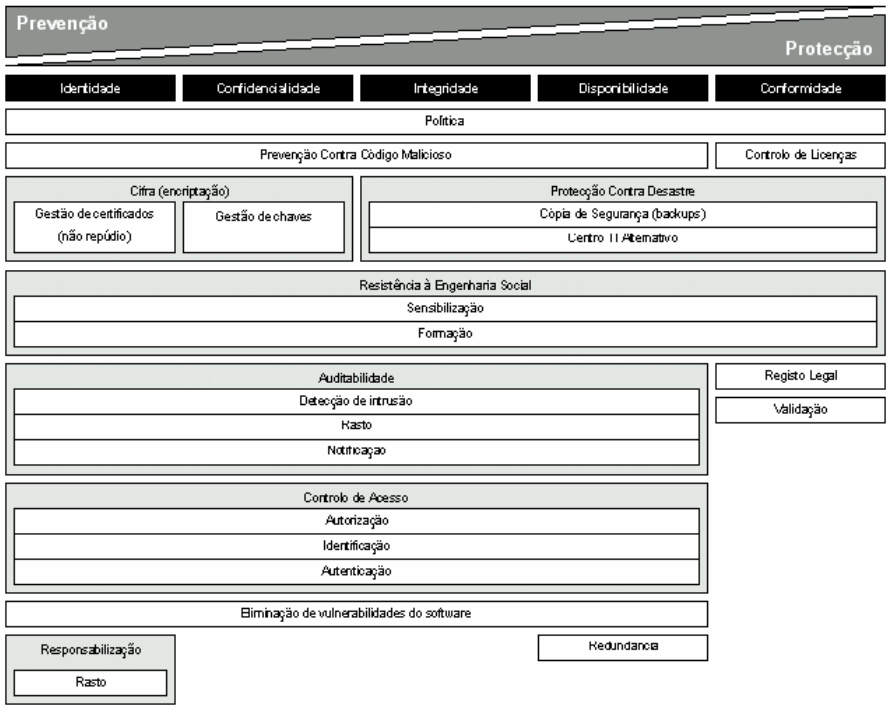


Fig. II-7: Arquitectura de Segurança dos Sistemas de Informação

Exemplo: após a definição da arquitectura alvo de alto nível para a segurança dos sistemas de informação, antes de adicionar uma *Extranet* nova, o responsável pela segurança deverá desenhar o diagrama correspondente à arquitectura alvo para a rede em matéria de segurança. Esta arquitectura de baixo nível é composta pelo diagrama de ligação dos dispositivos (*firewalls*, *routers*, *proxies*, etc.), pela descrição das suas funções à luz da arquitectura de alto nível e pela designação das diversas zonas da rede (*Internet*, *Intranet* dos parceiros, *Intranet* do grupo, rede privada, zona desmilitarizada, etc.)

A definição da arquitectura alvo para a segurança dos sistemas de informação, assente numa estratégia global, irá permitir que as diversas intervenções, mesmo que pontuais, sejam consistentes com os objectivos definidos da segurança e contribuam para aumentar a sua maturidade.

Abordagens ao Controlo de Riscos

A selecção do tipo de controlo apropriado ao tratamento dos diversos riscos que ameaçam a Empresa pode ser auxiliada pela produção de um mapa de riscos, ou seja, pela representação dos riscos num gráfico bidimensional em função da sua frequência de concretização (num dos eixos) e impacto (no outro eixo).

A partir do mapa de risco assim criado, será possível implementar uma estratégia para a segurança, ordenando os riscos por prioridade e identificando o controlo adequado a cada um, pela aplicação de regras baseadas nas áreas do mapa.

Exemplo: na Fig. II-8 são representadas duas estratégias distintas, baseadas em mapas de risco.

A estratégia indicada no mapa do lado esquerdo corresponde à prioridade conferida aos controlos pela

área correspondente ao grau de risco (de muito alto até baixo risco).

A estratégia representada no mapa do lado direito define uma abordagem ao risco (evasão, redução, aceitação ou transferência) em função do quadrante do mapa em que este se encontre:

Q1 - Aceitação;

Q2 - Transferência (por exemplo, seguro);

Q3 - Redução (da frequência e impacto do risco);

Q4 - Evasão (redução da frequência de concretização do risco).

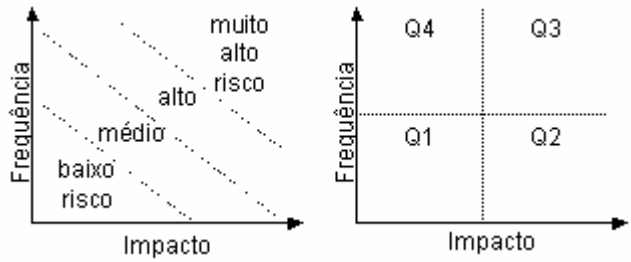


Fig. II-8: Regras baseadas no mapa de risco

Maturidade

A lógica subjacente à implementação dos controlos deve garantir, tanto quanto possível, a evolução da segurança da Empresa, sendo necessário para tal assegurar que a introdução de controlos básicos precede a introdução dos controlos mais sofisticados. Tal cuidado requer, por sua vez, a utilização de um modelo de maturidade, em que são definidos níveis de complexidade, à semelhança dos

degraus de uma escada, que deverão ser percorridos sequencialmente.

O modelo de maturidade anteriormente proposto assenta nas seguintes etapas:

1) definição de políticas e normas de segurança;
2) definição da arquitectura e dos processos da segurança;
3) implementação dos processos de suporte à inspecção, protecção, detecção e reacção;
4) realização de acções de sensibilização e de formação em segurança;
5) realização periódica de auditorias e testes à segurança;
6) implementação de processos de resposta reflexa;
7) validação do modelo de protecção e da sua implementação.

Segundo este modelo, as primeiras actividades do Programa de Segurança deverão ser dirigidas à criação de um corpo normativo onde serão definidas as regras de segurança a implementar na Empresa e definidos os alvos para a segurança nas diversas áreas. Em seguida, o Programa de Segurança deverá lidar com a componente humana desta problemática e com a implementação das ferramentas (tipicamente tecnológicas), após o que deverá promover a visibilidade, tanto das vulnerabilidades presentes nos sistemas de informação como dos incidentes registados. Por fim, a Empresa deverá encetar um esforço de validação para determinar o grau de conformidade da realidade com os alvos definidos para a sua segurança.

Análise Custo/Benefício

Na grande maioria das situações, o retorno sobre o investimento (ou *Return on Investment* - ROI) directo da segurança é difícil de determinar. Basta pensar no "*bug* do ano 2000" para perceber que os gastos em segurança pretendem evitar as despesas decorrentes da

inacção, pelo que a introdução de controlos é mais facilmente analisada em termos de custo/benefício, considerando como benefício o dano evitado, do que em termos de ROI.

A análise de custo/benefício de um controlo é realizada através da comparação directa do investimento (necessário à implementação) e do custo da sua manutenção com o valor do impacto da concretização (expectável) da ameaça associada ao controlo.

Quando a recomendação de controlos passa pelo cálculo da ALE (*Annual Loss Exposure*), apresentado anteriormente, a forma mais simples de determinar o benefício decorrente da introdução de um determinado controlo é através do cálculo da redução da exposição anual à perda, ou seja, do cálculo do ALE_b, utilizando para o efeito a seguinte variação das duas fórmulas apresentadas anteriormente:

$$R_b = (V\text{-}V_c) \times P$$

$$ALE_b = Valor \times R_b$$

Onde:

- R_b: redução da probabilidade de concretização da ameaça na Empresa no período de um ano, decorrente da introdução do controlo (expressa em ocorrências por ano).
- V: número que representa a vulnerabilidade da Empresa à ameaça (sem unidade).
- V_c: número que representa a redução da vulnerabilidade da Empresa à ameaça, após a introdução do controlo (sem unidade).
- P: probabilidade correspondente ao número médio esperado de vezes que a ameaça se irá concretizar por ano (expresso em ocorrências por ano).
- ALE_b: redução na perda monetária média expectável num ano, decorrente da introdução do controlo (expressa numa unidade monetária).

Exemplo: considerando o exemplo apresentado anteriormente em "Análise de Risco Quantitativa", o benefício da introdução de um sistema de supressão de fogo por CO_2 que permita a extinção de um fogo no *datacenter* sem danificar os equipamentos poderia resultar no seguinte valor novo para V:

V = 1,0 (normal) + 0,5 (da cantina) - 0,2 (do sistema de extinção)

$R_b = 0{,}01 \times 1{,}3 = 0{,}013$

$ALE_b = 300.000 \times 0{,}013 = 3{,}900$

Deste modo, a introdução do controlo representaria uma redução da exposição à perda de seis mil para três mil e novecentos Euros por ano.

Conclusão

Neste capítulo foram abordadas formas alternativas de analisar o grau de exposição da Empresa aos riscos e de selecção das medidas necessárias para os reduzir ou eliminar, em função do resultado dessa análise.

Nos próximos capítulos serão descritas algumas dessas medidas, designadas por controlos, bem como a sua implementação e gestão.

Capítulo III - Áreas da Segurança Empresarial

Este capítulo pretende descrever as principais áreas em que se inserem os controlos de segurança. Contém uma listagem dos principais aspectos a que qualquer responsável terá de se dedicar durante a implementação de um Programa de Segurança, sob pena deste não ser compreensivo nas suas medidas de prevenção e protecção. Pretende-se com este capítulo listar as características dessas áreas e chamar a atenção do leitor para as suas particularidades.

Segurança da Informação

O responsável pela implementação da segurança dos sistemas de informação (SI) na Empresa tem, como primeira missão, e mais importante, a garantia da segurança da informação que protege. Esta garantia é conseguida mediante a utilização de vários instrumentos, que deverão abarcar as diversas áreas apresentadas em seguida.

Política, Normas e Procedimentos

Estes são os mecanismos formais que definem os objectivos da organização em termos de segurança, bem como as acções a empreender com vista à concretização dos mesmos. Encontram-se mais desenvolvidos em “Os Documentos da Segurança”, no capítulo “Criação do Plano de Segurança”, mas, como peças centrais que efectivamente são, serão aqui abordados.

Em si, este corpo doutrinário encerra os grandes objectivos de segurança da organização e define os principais eixos em torno dos quais se desenvolverão todas as actividades de prevenção e protecção. Estes documentos incluem os grandes objectivos a conseguir através do Plano Global de Segurança, influenciando desta forma a definição das linhas de conduta a desenvolver e implementar para os atingir.

O responsável pela segurança dos SI deverá, por um lado, garantir o cumprimento dos preceitos contidos neste conjunto de documentação e, por outro, certificar-se de que existe uma correcta e continuada actualização destes documentos, sob pena de poder estar a realizar esforços inadequados. Para além disso, a tarefa de actualização evitará a obsolescência dos documentos, evitando a sua perda de valor: afinal, uma má política poderá ser pior do que não ter política.

Propriedade da Informação

Um passo essencial na definição e implementação de medidas eficazes de salvaguarda é a existência de uma clara identificação dos proprietários da informação da organização. Ao determinar os responsáveis pelos dados existentes nos SI da Empresa, o responsável pela segurança terá interlocutores claramente identificados com quem poderá definir as necessidades reais de segurança, evitando aplicar medidas genéricas a toda a informação da Empresa, medidas essas muitas vezes desajustadas da realidade.

Classificação da Informação

Uma vez identificados os responsáveis pela informação existente nos SI, esta poderá mais facilmente ser classificada de acordo com a sua sensibilidade e, posteriormente, protegida de acordo com essa classificação. Deve-se notar que a classificação não constitui um fim em si mesmo, mas antes um meio que permite definir proce-

dimentos para a gestão da informação, como por exemplo a sua destruição, armazenamento ou transporte.

A classificação poderá ser tão simples como a separação dos dados em "públicos" e "privados", ou poderá conter um maior grau de complexidade, dividindo a informação em vários níveis (ver, também, "Acordos de Nível de Serviço" no capítulo "Criação do Plano de Segurança"). Este processo deverá ser orientado por definições claras dos diferentes graus de sensibilidade da informação, reconhecidos pela Empresa, bem como pela determinação exacta dos responsáveis pela classificação. Estas definições, que devem ser feitas antes do início da classificação, servirão para evitar a acumulação de documentos "sobre-classificados", gerando uma enorme sobrecarga em termos de gestão. Por outro lado, também deverão ser determinadas as condições de desclassificação da informação, ou seja, as condições segundo as quais a informação descerá na escala de classificação. Esta descida pode ser motivada pela passagem do tempo ou poderá estar relacionada com outros factores, tais como o lançamento de produtos ou serviços, entre outros.

Para que este processo seja viável, é importante perceber quais as consequências para a organização da divulgação, alteração ou eliminação não autorizadas dos dados classificados. Somente através da interacção com as pessoas directamente responsáveis pela informação da Empresa se poderão estabelecer estas consequências e criar graus apropriados de classificação.

Obviamente, este esforço de nada servirá se não for seguido de medidas de protecção adequadas aos níveis de classificação atribuídos. Como tal, deverão aplicar-se os princípios apresentados anteriormente no capítulo "Teoria da Segurança", nomeadamente de protecção concêntrica e em profundidade, criando, deste modo, várias camadas de segurança que, mesmo com falhas parciais, continuem a proteger os dados.

Este esforço de classificação permite desenvolver níveis de protecção idênticos para informação com os mesmos requisitos de segu-

rança, permitindo a sua concentração, o que irá maximizar o efeito dos esforços de protecção. Nos casos em que não seja possível agrupar a informação com as mesmas necessidades de segurança, a classificação permite definir padrões de protecção, claros e inequívocos, para as várias categorias de classificação.

Exemplo: toda a informação classificada de "vital" deverá ser objecto de controlo de acessos, autorizado superiormente pela Administração.

Confidencialidade

A vantagem competitiva das empresas assenta muitas vezes na informação que detêm e na capacidade de controlar a sua divulgação (os exemplos mais flagrantes poderão ser as empresas de investigação e desenvolvimento, ou as metodologias específicas de uma organização). Deverão, por isso, existir mecanismos que garantam a confidencialidade da informação, mas que não impeçam o acesso atempado de pessoas autorizadas à mesma. Os requisitos de confidencialidade são claramente influenciados, senão mesmo definidos, pela classificação aposta à informação.

Integridade

A integridade é um dos aspectos vitais a garantir relativamente aos dados armazenados, processados e transmitidos pelos SI.

Todo o valor da informação reside na fiabilidade: o erro de uma vírgula (ou ponto decimal) poderá comprometer a integridade de um enorme volume de dados e poderá acarretar prejuízos significativos. Como tal, deverão existir sistemas de validação da informação existente. Dependendo do grau de importância da informação, estes poderão ser automáticos (como sejam regras automáticas de validação de introdução), ou poderá ser necessário implementar processos manuais de validação. Poderão, por exemplo, ser instituídos

procedimentos de revisão, por amostragem, da integridade dos dados existentes.

A integridade é igualmente vital para a recuperação de informação perdida, uma vez que o valor das cópias que não apresentam garantias de integridade é praticamente nulo.

A classificação da informação em termos de integridade visa adequar o custo das medidas de protecção ao impacto das perdas esperadas (ou possíveis).

Disponibilidade

O acesso atempado à informação é vital e dele depende a prossecução dos objectivos da Empresa. Possuir a informação necessária mas não a ter disponível no momento adequado equivale a não possuir qualquer informação.

As medidas de protecção dos dados deverão contemplar aspectos que facultem o acesso aos mesmos. Porém, para além disso, deverão ser capazes de fazer a distinção entre acessos autorizados e acessos não autorizados.

Acima de tudo, é importante conseguir equilibrar a necessidade de acesso à informação com a necessidade de preservação da confidencialidade da mesma. As medidas de protecção utilizadas não deverão expor os dados (permitir o acesso indevido) nem impedir ou dificultar significativamente o acesso (devido) a esses dados. Porém, podem surgir situações em que a posse e o acesso à informação é mais importante do que a manutenção da sua segurança.

Exemplo: em caso de uma emergência médica, durante uma catástrofe natural, poderá ser necessário fornecer acesso a informação clínica ao pessoal médico deslocado para o local do desastre, sem que este seja submetido às formalidades de segurança estabelecidas.

Política de Dados

Uma política de salvaguarda (*backup*) e recuperação de dados adequadamente elaborada e executada protegerá a organização contra a perda de informação devida a falhas de hardware, defeitos de software, erros humanos, intrusos, sabotagem e desastres naturais, podendo igualmente ser utilizada para suporte ao arquivo (histórico) de dados. Para que esta solução cumpra com os seus objectivos, é necessário que seja suportada por mecanismos organizacionais (procedimentos, processos, e outros) que se ocupem com a informação, sendo, pois, fundamental desenvolver uma política formal de gestão de dados.

Esta política permite obter dois resultados significativos: em primeiro lugar, define os requisitos da organização em termos de protecção e integridade da informação e, em segundo, proporciona a concretização desses requisitos através da sua aplicação, consubstanciada em procedimentos e ferramentas adequados.

O seu conteúdo deverá abordar os prazos de manutenção dos diferentes tipos de dados (o que implicará, naturalmente, a existência de procedimentos de classificação da informação), bem como descrever os procedimentos para o arquivo e destruição. Ao falar de dados, não nos referimos apenas a ficheiros electrónicos (incluindo correio-electrónico), mas também a toda a informação em suporte físico: lembremo-nos que um plano de continuidade do negócio adequado deverá identificar os relacionamentos e interdependências entre as informações nos mais variados suportes, sem esquecer o conhecimento humano que as permite processar. Por outro lado, é essencial contemplar medidas que previnam a obsolescência dos suportes mecânicos de leitura de dados – quanto tempo mais iremos encontrar *drives* ZIP no mercado?

Uma política de dados permitirá, ainda, reduzir a duplicação de dados, rentabilizar os investimentos em suportes de armazenamento e realizar poupanças efectivas em termos de custos de gestão. O seu ciclo de vida pode, de uma forma resumida, ser apresentado nos seguintes pontos:

- Criação de uma equipa: esta deverá conter não só membros do departamento de TI, mas também utilizadores, juristas e representantes de todas as partes envolvidas;
- Inventariação de recursos e da respectiva utilização: a infraestrutura deverá ser analisada e classificada, assumindo que nenhum sistema é imune a ataques, acidentes ou falhas;
- Levantamento de padrões de utilização: deverá olhar-se para o modo como as tarefas são efectivamente realizadas e não como em teoria deveriam ser feitas, de modo a identificar os padrões reais de utilização dos sistemas;
- Estabelecimento dos fundamentos da política: as regras isoladas que forem definidas não podem ser encaradas como garantias efectivas de sobrevivência, decorrendo a protecção eficaz da sua combinação;
- Teste de ferramentas *Storage Resource Management* (SRM) e análise de suportes de armazenamento: procurar soluções que permitam aplicar a política da forma mais eficaz e racional possível;
- Definição da política: criação formal e aprovação ao nível da Administração;
- Divulgação da política: deverão ser comunicadas aos destinatários as razões que levaram à sua adopção, as consequências da sua entrada em vigor, os comportamentos a adoptar, etc.;
- Entrada em vigor da política: implementação dos mecanismos seleccionados;

- Manutenção da política: monitorização e aperfeiçoamento da solução em funcionamento, sem nunca perder de vista os reais objectivos da organização.

Os tópicos da confidencialidade, integridade e disponibilidade encontram-se intimamente ligados no que concerne a protecção da informação, quer esta seja física ou lógica. Uma falha num destes elementos compromete os restantes, pelo que os controlos a implementar no Plano Global de Segurança deverão ter em conta o íntimo relacionamento destes aspectos, bem como a complexidade de gestão a eles associada. Assim, através da correcta aplicação das soluções apropriadas, estes três vectores serão garantidos.

Os mecanismos a utilizar deverão basear-se na "filosofia" de segurança vigente na Empresa, consubstanciada na política, nas normas e nos procedimentos definidos para a segurança, bem como nos requisitos definidos pelos proprietários da informação. Estes controlos, enquadrados desta forma, poderão materializar-se, por exemplo, sob a forma de acordos de nível de serviço para a segurança, abordados mais adiante neste livro (ver "Acordos de Nível de Serviço", no capítulo "Criação do Plano de Segurança").

Todos os controlos que possam vir a ser introduzidos para a garantia das necessidades citadas deverão dar resposta às particularidades das várias áreas da segurança empresarial. Os capítulos que se seguem apresentam essas áreas e respectivas características.

Segurança Física

O ambiente físico no qual a Empresa opera pode constituir um dos mais importantes elementos no que diz respeito à salvaguarda da informação.

Muita da tecnologia que vimos em filmes futuristas ainda não é realmente praticável, apesar de já existir a possibilidade de capturar indevidamente dados à distância, com relativa facilidade, a partir das radiações emanadas pelos monitores dos computadores, atra-

vés dos cabos de alimentação eléctrica, ou das placas de rede *WLAN*. Para a grande maioria das empresas, estes perigos não serão realistas, mas existem outros riscos físicos para os quais as organizações devem estar alertadas.

Áreas

Em zonas densamente povoadas, como sejam os centros urbanos, a questão da escolha da localização da Empresa pode estar altamente condicionada. Porém, a importância da definição de áreas, no seio da própria Empresa, contribui decisivamente para a construção de ambientes seguros. Existem erros que, fruto de condicionamentos de espaço, podem efectivamente fragilizar a capacidade de protecção da informação.

Os componentes críticos de armazenamento, processamento ou transmissão não deverão encontrar-se demasiado expostos, nem deverão ser de acesso demasiado fácil. Não é necessário criar *bunkers* mas, por exemplo, poderá bastar evitar a instalação de componentes sensíveis, como sejam arquivos, ou bastidores de dados, em zonas de acesso público (como corredores).

A segurança física deverá ser pensada em moldes concêntricos e de profundidade, com vista a incrementar os níveis de protecção contra acessos não autorizados. Segundo esta lógica, os bens mais preciosos deverão encontrar-se mais perto do centro das instalações, obrigando à passagem por diversos níveis de validação. Pelo contrário, os componentes menos valiosos, ou mais facilmente substituíveis, poderão ficar em zonas periféricas, menos protegidas, mas nunca dispensando por completo um qualquer tipo de salvaguarda.

Os diferentes níveis de validação devem, igualmente, ser proporcionais à informação que protegem.

Exemplo: O acesso a uma sala de processamento de dados é protegido por um leitor de cartões magnéticos. Dentro dessa sala, o acesso à zona das consolas de Adminis-

tração dos sistemas centralizados já requer, para além do cartão magnético, um PIN numérico. Por outro lado, o acesso à sala dos servidores já poderá obrigar ao registo num livro de acesso, bem como à utilização do cartão e do PIN.

Localização dos Centros de Dados

Segundo a proposição atrás apresentada, a localização dos centros de dados, ou dos arquivos de informação crítica para a Empresa, deverá ser cuidadosamente considerada. Numa situação em que se está a planear de raiz a construção de um edifício, existem várias linhas de orientação que deverão ser seguidas para a correcta localização e configuração de um centro de processamento de dados (CPD).

De seguida apresentam-se algumas:

- O CPD não deverá ficar nem no piso térreo nem no último piso do edifício;
- No caso de edifícios térreos, o centro deverá ficar localizado na zona mais resguardada possível, i.e., longe de vias de circulação pública;
- Não deverão existir quaisquer acessos directos do exterior (janelas, portas, respiradouros, etc.);
- Os acessos existentes deverão poder ser facilmente monitorizados;
- Não deverão existir condutas de águas ou de esgotos nas imediações (nem por cima nem por baixo) dos centros de dados;
- As instalações deverão ser dotadas de chão e tecto falsos, para a passagem das condutas necessárias à alimentação energética e processamento de atmosfera;

- Deverão existir sistemas de alimentação eléctrica redundantes;
- Os sistemas de detecção e combate a incêndios deverão ser apropriados (ou seja, não devem ser instalados *sprinklers* de água mas antes sistemas de supressão por gás inerte).

Estas orientações, se seguidas, permitem a criação de um centro de TI conforme com as mais exigentes normas de segurança, nacionais e internacionais, e deixaria qualquer responsável pela segurança perfeitamente realizado.

Porém, nem todas as situações permitem o cumprimento das orientações apresentadas. No caso de instalações já existentes, ou de quaisquer outros condicionalismos, surge a necessidade de fazer o melhor possível com o que já existe. Nesses casos, uma boa dose de bom senso e de sensibilidade para os factores que podem afectar adversamente a informação serão suficientes para realizar os ajustes necessários e para conseguir elevar a qualidade das condições de localização do CPD. Poderá, nalguns casos, ser suficiente instalar cofres ignífugos em salas de acesso mais restrito para protecção de dados mais sensíveis.

Controlo de Acessos

O controlo de quem entra e de quem sai das instalações é um aspecto particularmente importante da segurança física. Não basta ter um guarda à entrada e obrigar todos os visitantes a registarem-se. É fundamental ter a certeza, por exemplo, de que os visitantes não levam material da Empresa sem autorização expressa do responsável por esse equipamento. Para além disso, são necessárias medidas adicionais para garantir que as soluções de controlo não são ultrapassadas, evitando situações em que, por comodismo, uma porta é encravada aberta, por exemplo.

Mas o controlo de acessos não se resume a uma portaria com guardas e, eventualmente, um sistema de vídeo em circuito fechado. Este controlo deve ser alargado a todas as áreas sensíveis,

nomeadamente aos centros de dados e aos arquivos centrais, e deverá ser abrangente, na medida em que não devem existir excepções.

Na sala de servidores da organização, por exemplo, poderão ser registados os acessos de todos os operadores e administradores, incluindo as suas horas de entrada e de saída. Casos haverá em que, para além de um sistema automático de controlo, como por exemplo um leitor de cartões magnéticos, fará sentido a existência de um livro de registo de acessos, onde todos deverão inserir a data e hora de entrada e saída, bem como uma rubrica para autenticação do registo.

Existem igualmente soluções, baseadas em tecnologia, que permitem definir, de forma automatizada, horários de acesso a determinados locais, e que podem ser implementadas com um impacto relativamente reduzido sobre o funcionamento normal da organização.

Nenhuma destas medidas, porém, fará sentido sem o devido acompanhamento. Quantos são os casos conhecidos de empresas em que a segurança no átrio de entrada serve apenas de "decoração"? O registo dos acessos deverá ser verificado pelo responsável pela segurança, em particular o dos acessos às zonas mais sensíveis da organização, e quaisquer situações mais duvidosas deverão ser prontamente questionadas e esclarecidas. Para tal será necessário sensibilizar os colaboradores da Empresa para que, também eles, sejam parte do mecanismo de segurança física responsável pela detecção de intrusos.

Eliminação de Resíduos

Os resíduos são o que o próprio nome indica: restos, lixo, coisas que deixaram de possuir interesse e que, como tal, são eliminadas. A sua eliminação, porém, não é frequentemente a mais indicada e acaba por criar potenciais compromissos à segurança da Empresa.

Tal como todos temos cuidado ao destruir a carta do nosso banco com o código de um cartão de débito, também deveremos dedicar igual atenção ao modo como a informação sensível é eliminada.

Uma "disciplina" muito popular entre os *hackers*, conhecida por "*dumpster diving*", consiste, muito resumidamente, em vasculhar os contentores de lixo de uma empresa em busca de informação. E os resultados são, muitas vezes, preciosos: desde listas de utilizadores com dados pessoais, listagens de números de telefone directos, organigramas funcionais, impressões de configurações de equipamento, de tudo se encontra num caixote de lixo. E muito desse "lixo" poderá constituir uma valiosa fonte de informação para um ataque futuro, quer informático, quer físico, através de engenharia social, por exemplo.

Rasto

O rasto é, resumidamente, o registo de qualquer actividade monitorizada nas instalações de uma organização. Este registo pode ser composto pelos mais diversos elementos, quer sejam gravações vídeo, áudio, registos biométricos, de cartões de acesso (de banda magnética ou *smart cards*), etc.

É o rasto que permite reconstituir um qualquer evento, revelando quem fez o quê, quando e como. Como tal, todos os registos gerados pelas medidas de protecção física devem ser arquivados por um determinado período, permitindo reconstituir, nesse espaço de tempo, o rasto de todos os indivíduos presentes nas instalações e, dessa forma, detectar actividades não autorizadas, quebras de segurança ou, mais simplesmente, acções suspeitas.

Somente através do cruzamento dos vários rastos criados pelas diversas formas de segurança física conseguirá o responsável, ou a equipa de segurança, investigar e, eventualmente, evitar potenciais compromissos de confidencialidade, integridade ou disponibilidade da informação.

Segurança do Pessoal

A segurança tende, na grande parte dos casos, a ocupar-se principalmente com as facetas física e tecnológica dos problemas, devotando particular atenção às soluções técnicas para as fragilidades inerentes à tecnologia. A mitigação das vulnerabilidades e das ameaças tende, por seu lado, a reflectir a utilização de meios tecnológicos, melhor ou pior enquadrados nas necessidades do negócio. É nestas áreas que os especialistas em segurança investem mais tempo (e dinheiro), especializando-se nesta disciplina restrita e altamente especializada da segurança dos sistemas de informação.

Como consequência, constata-se frequentemente que muito pouca relevância é conferida a um dos elos mais importantes da cadeia: a componente humana.

São as pessoas que interagem diariamente com os sistemas, que têm acesso à informação neles contida, que condicionam o processamento dessa mesma informação, que a gerem. E, também muitas vezes, são as próprias pessoas a principal ameaça a esses mesmos sistemas.

As estatísticas realizadas na área da segurança dos SI têm revelado uma tendência continuada, se não mesmo crescente, para a existência de um grande número de ataques consumados por *insiders*, ou seja, por elementos internos à própria organização. Esses ataques podem ser acções deliberadas e planeadas com antecipação e com o objectivo de provocar grandes prejuízos à organização, ou, simplesmente, podem ser o resultado de acções mal executadas, de erros humanos. Mas, apesar destas evidências, a ênfase continua a ser dada à tecnologia e às soluções que esta pode proporcionar, em detrimento de acções de sensibilização e formação junto dos utilizadores.

É a esta acção pedagógica que nos iremos dedicar de seguida.

A pedagogia da segurança é, provavelmente, uma das tarefas mais sensíveis sob a alçada do responsável pela segurança da Empresa.

Não por se tratar de um tema extraordinariamente complexo, mas por implicar a gestão de sensibilidades e percepções distintas e a interacção com personalidades diferentes.

De facto, e independentemente da dimensão da organização em causa, dificilmente se encontrarão dois colaboradores iguais. No primeiro capítulo deste livro, "Teoria da Segurança" foram tipificados e caracterizados genericamente diferentes grupos de intervenientes e destacados os seus aspectos mais distintivos. Aqui iremos, por outro lado, dedicar-nos às acções que poderão ser empreendidas junto dos colaboradores, com vista a criar um ambiente de utilização dos sistemas de informação que, por si só, seja um factor influente na manutenção dos níveis de segurança pretendidos.

Recrutamento

A fase de recrutamento é uma altura crítica no processo de sensibilização do potencial colaborador para a filosofia da Empresa, incluindo a componente de segurança desta.

Se cargos há em que a segurança dos SI é um componente discreto, quase imperceptível, outros existem em que poderá constituir o ponto central das funções a desempenhar. Estas diferenças deverão ser claramente identificadas e comunicadas ao potencial novo colaborador na fase de recrutamento. As componentes de segurança associadas à função para a qual concorre deverão ser-lhe explicadas, mesmo que se resumam à política de "secretária limpa", pois o candidato deverá conhecer todas as "cartas com que terá de jogar".

De uma forma geral, mas particularmente no caso de funções extremamente sensíveis, deverá equacionar-se a possibilidade de se realizar um *background check*[7]: este poderá ser tão simples

[7] Existem, inclusivamente, empresas de recursos humanos no mercado que realizam o serviço de verificação de currículos e das referências apresentadas pelo candidato.

quanto o pedido de apresentação de comprovativos da formação e cargos existentes no *curriculum vitae*, ou poderá incluir contactos com antigos empregadores.

Esta verificação de antecedentes terá de ser cuidadosamente equilibrada com a função em causa, de modo a evitar situações desagradáveis, tanto para o potencial empregador como para o potencial empregado. Por outro lado, caso não exista qualquer tipo de verificação, a Empresa estará a confiar somente na palavra do candidato: se, na maioria dos casos, esse facto pode não representar qualquer problema, noutros há a hipótese real de surgirem surpresas desagradáveis.

Aquando da contratação de um novo colaborador, e na fase inicial de introdução deste às suas funções, deverá ser dedicado algum esforço à integração do novo elemento na filosofia de segurança da Empresa. Este enquadramento deverá ser realizado através da explicação da política de segurança, devendo igualmente ser-lhe comunicadas quais as acções aceitáveis, ou seja, quais as boas práticas em vigor na organização.

Se existir uma "Política de Uso Aceitável" formal na Empresa, esta deverá ser lida pelo novo elemento, que a deverá assinar, assinalando deste modo a sua aceitação. Caso não exista documentação formal, mas antes orientações informais sobre o que constitui, ou não, o uso aceitável dos SI da Empresa, estas deverão ser comunicadas ao novo elemento, que deverá assinar uma declaração em como foi instruído sobre o que pode, ou não pode, fazer. Esta aceitação inicial das "regras do jogo" leva a que mais tarde não possam surgir afirmações de alegado desconhecimento, que poderão conduzir a situações no mínimo complicadas.

Como vimos, as questões levantadas levam, então, à necessidade de colaboração entre o Departamento de Recursos Humanos, ou a pessoa responsável pela contratação de novos colaboradores, e o responsável pela segurança da Empresa que, em certos casos, poderá inclusivamente participar activamente no processo de selecção de novos funcionários.

Documentação

Política, normas e procedimentos. Nunca é demais frisar a importância de um corpo documental coeso, actual e apropriado.

Ao criar uma política de segurança clara e explícita, a Empresa está a fixar os seus objectivos nesta área, sem (idealmente) margem para dúvidas. Esta política, para além de constituir, juntamente com o Plano Global de Segurança, o fio condutor da actuação da Empresa nesta matéria e de representar o ponto de partida para toda a documentação de apoio subsequente (normas e procedimentos), deverá servir de orientação e referência para todos os elementos da organização, no que concerne à segurança.

Portanto, um dos primeiros, e mais essenciais, passos a dar no que respeita ao enquadramento dos utilizadores, deverá ser a adequada divulgação da Política de Segurança da Empresa.

Esta medida poderá ser iniciada por um memorando interno, distribuído a todos os colaboradores, com uma cópia integral da Política de Segurança da Empresa, mas não deverá ficar por aí. Esta leitura isolada poderá, em muitos casos, ser insuficiente. Se uma frase como "*Toda a informação armazenada, transmitida ou processada pelos sistemas de informação da <Empresa> é propriedade da <Empresa>*" poderá não levantar muitas dúvidas, uma afirmação como "*A <Empresa> envidará todos os esforços para garantir a privacidade da sua informação proprietária*" irá, provavelmente, suscitar todo o tipo de interrogações: qual é a informação proprietária da Empresa? O que se entende por "todos os esforços"? Que impacto é que esta política tem sobre a minha privacidade? Quais são as *minhas* garantias?

O exemplo apresentado chama a atenção para dois aspectos vitais: por um lado, é imperativo que uma política empresarial não seja sujeita a interpretações ambíguas e que, descontextualizadas, possam levar a conclusões erradas. Por outro, a leitura da política de segurança por parte dos utilizadores deve constituir o início, e não o fim, da introdução destes à filosofia da Empresa.

Depois de divulgada individualmente, a política de segurança poderá, por exemplo, ser apresentada na Intranet, contendo comentários às suas regras. Para além disso, o responsável pela segurança empresarial deverá estar sempre disponível para o esclarecimento de quaisquer dúvidas que a política de segurança ou as normas/procedimentos possam levantar. O importante é apresentar a política da Empresa de uma forma enquadrada e contextualizada.

Não deverão restar dúvidas aos utilizadores sobre qual é a atitude da organização em relação à segurança: se todo o correio-electrónico for sujeito a inspecção de conteúdo, este facto deverá ser do conhecimento geral e não deve, nunca, ser ocultado aos utilizadores.

Boas Práticas

Todas as organizações possuem, em moldes formais ou informais, orientações que podem ser entendidas como as boas práticas de utilização dos recursos disponíveis. Este conjunto de orientações deverá ser comunicado aos colaboradores da Empresa, de forma a estabelecer claramente os limites do que é, ou não, aceitável.

É sempre preferível, mesmo nos casos em que não exista uma orientação formal, comunicar essas balizas de comportamento aos utilizadores, em vez de deixar as decisões desse campo ao critério individual de cada um.

Se essas linhas de conduta existirem num documento formal, esse deverá ser lido e assinado pelos colaboradores o mais cedo possível, de preferência no acto da contratação. Caso sejam um conjunto de regras informais, partes integrantes da cultura da Empresa, o responsável pela segurança deverá envidar esforços no sentido de esclarecer essas regras e de as manter actualizadas.

Esta questão tem particular importância no que concerne a utilização do correio-electrónico. De facto, este meio de comunicação é, claramente, o veículo de transmissão de dados com maior visibilidade no panorama actual. Caso não sejam definidas as boas práti-

cas de utilização deste meio, a Empresa corre sérios riscos de se deparar com um consumo desmedido dos seus recursos de transmissão de dados (largura de banda, etc.) na comunicação de mensagens de cariz puramente pessoal e, por vezes, arriscando-se à transmissão de informações confidenciais.

Não se pretende aqui defender uma política rigorosa de restrição da utilização do correio-electrónico – essa decisão dependerá, sempre, das circunstâncias funcionais da Empresa –, mas antes alertar para a necessidade imperiosa de estabelecimento de limites: será aceitável enviar e receber mensagens pessoais com anexos volumosos? Será aceitável enviar e receber mensagens pessoais de cariz sexual? Será aceitável a transmissão de mensagens contendo informação proprietária da Empresa? O correio-electrónico deverá ser exclusivamente utilizado, sem excepções, para o desempenho das funções profissionais do utilizador?

Estas questões deverão obter resposta no desenvolvimento de um conjunto de regras, mais alargado, que constituirão as boas práticas da Empresa.

Formação

Com a regularidade que venha a ser definida como necessária (dependendo do tamanho da Empresa, do número de colaboradores, da quantidade de pessoal dedicado à segurança, etc.), deverão ser preparadas, em estreita coordenação com o Departamento de Recursos Humanos, acções de formação sobre a segurança.

Longe de seminários exaustivos e demasiado técnicos sobre segurança dos SI, estas deverão ser acções em que se instruam os utilizadores sobre como realizar as tarefas quotidianas que lhes competem, de modo a não afectar a segurança dos SI. Deverão ser apresentadas de forma genérica as tecnologias em utilização na Empresa, os seus objectivos, eventualmente a forma como os atingem, e as implicações que essas medidas de protecção têm para quem as utiliza. Idealmente, a segurança deverá ser também incor-

porada nos conteúdos programáticos das acções de formação de outras áreas.

Sensibilização

Para além das acções de formação dedicadas a aspectos específicos da segurança dos SI, com impacto sobre os utilizadores, deverão realizar-se acções de sensibilização sobre questões concretas.

Os temas poderão ser propostos pelos próprios utilizadores, através de um sistema de sugestões (por exemplo, através da Intranet - a adesão poderá ser surpreendente!), poderão resultar da observação directa dos problemas quotidianos mais preponderantes na Empresa (por exemplo, vírus, ou *spam)*, ou poderão estar relacionados com as questões fundamentais da segurança na organização.

Um exemplo flagrante, e provavelmente o mais típico, é o das palavras-passe. Uma acção de sensibilização poderá dedicar-se a estes mecanismos de autenticação, explicando qual o comprimento necessário, a respectiva validade, e a importância da sua salvaguarda. Poderão igualmente ser apresentadas formas simples de criar e memorizar palavras-passe eficazes e exemplificar as más escolhas (datas de nascimento, etc.).

Uma outra questão importante, que deverá ser abordada, é a da "engenharia social".

A engenharia social (*social engineering*) pode ser definida, de forma simples, como o conjunto de acções que, unicamente através da interacção humana, levam ao compromisso de informação confidencial. A interacção pode ser levada a cabo local ou remotamente.

Infelizmente, existem inúmeros exemplos de ataques compostos, principal ou exclusivamente, por actividades de engenharia social. Faz parte da natureza humana o espírito de entreajuda e essa tendência é por vezes agravada em ambientes laborais. Se, por exemplo, alguém telefonar a um utilizador, identificando-se como um

colega de outro departamento que precisa urgentemente de aceder a determinada informação, sob pena de ser despedido, a tendência instintiva do utilizador será ajudar. Alternativamente, o ataque pode assumir a forma de alguém que se identifica como um elemento do departamento de SI que necessita validar os dados de autenticação dos utilizadores do departamento financeiro. Ou, então, um contacto do fornecedor de acesso à Internet que precisa de qualquer elemento. Ou então... as possibilidades são inúmeras.

Eis um exemplo real.

Recentemente, um dos autores deste livro teve a necessidade de obter os dados (nome de utilizador e palavra-passe) da conta de gestão de um acesso dedicado à Internet de uma empresa.

Ligou para o operador de telecomunicações da Empresa em causa e, em pouco tempo, ficou a saber quem era o respectivo gestor de conta, bem como os seus contactos.

O passo seguinte, naturalmente, foi contactar o gestor, junto de quem se identificou como sendo um novo elemento da Empresa, responsável pela gestão de redes de comunicações. Informou o agente comercial da sua necessidade, fundamentou-a com o argumento de precisar de configurar vários parâmetros, e solicitou que a informação lhe fosse transmitida. O gestor de conta argumentou que a informação era confidencial e que já havia sido enviada para a Empresa, mas o contra-argumento foi o de que a Empresa estava mal organizada e as alterações eram urgentes. Assim, solicitava-se que os dados de acesso fossem comunicados por correio-electrónico (para um endereço particular) ou, por telefone, para um número de telemóvel.

Ao fim de alguma insistência (foi difícil para o gestor de conta obter os dados em questão), e depois de uma troca de mensagens de *e-mail* (sempre a partir da conta particular), o autor deste livro recebeu, por telefone, a informação pretendida.

O telemóvel utilizado podia ter sido qualquer um, acabado de comprar e não registado, e a conta de *e-mail* poderia ter sido acabada de criar com dados fictícios, utilizando um acesso gratuito à Internet, disponível nos supermercados. Ou seja, com meia dúzia de telefonemas, argumentos convincentes e alguma paciência, foi obtida a informação necessária para, por exemplo, encerrar as comunicações de dados de uma empresa. A ânsia de ajudar, a urgência em resolver o problema e a vontade de "satisfazer o cliente", todas contribuíram para que esta situação se verificasse.

Felizmente, as intenções por detrás deste exemplo eram legítimas, mas o autor aproveitou a situação para ver até que ponto seria possível obter este tipo de informação, extremamente sensível, sem ter de apresentar qualquer prova. E conseguiu-o.

Casos como este sucedem-se diariamente, em todo o mundo. Se, nalguns casos, tudo pode não passar de uma situação legítima, outros casos haverá em que alguém se queira aproveitar da boa-vontade alheia para fins menos apropriados.

Como responder a situações como esta? Não bastará definir um procedimento bem explícito sobre como lidar com pedidos de informação externos, se bem que este deva existir e deva ser o mais exaustivo possível. É importante alertar os utilizadores, particularmente aqueles que lidam diariamente com elementos externos à Empresa, para este tipo de ataques e para as formas de os reconhecer e de lidar com eles.

Se o procedimento deve conter instruções claras para a verificação da identidade dos interlocutores, locais ou remotos, a sensibilização dos utilizadores para esta questão levará a que estes exerçam o seu sentido crítico, tentando detectar atitudes suspeitas ou pedidos inusitados.

Segregação de Responsabilidades

Tal como o velho adágio nos indica, nunca é bom "colocar todos os ovos no mesmo cesto". Esta frase feita tem aplicação em todos os aspectos da nossa vida e igualmente no campo da segurança.

O objectivo da segregação de responsabilidades não é o de evitar que alguém venha a deter demasiado poder sobre qualquer aspecto da Empresa, mas antes o de criar mecanismos de salvaguarda que evitem situações que, mesmo inocentes, possam afectar adversamente o negócio, requerendo sempre a participação de, pelo menos, duas pessoas para completar qualquer processo crítico para a Empresa.

Assim, deverá evitar-se a atribuição a uma única pessoa de funções vitais para a organização, devendo sempre tentar distribuir-se essas funções por dois, ou mais, colaboradores. Como seres humanos que somos, ninguém está isento de um engano. Ao concentrar actividades críticas numa única pessoa, a Empresa estará a potenciar a possibilidade de falhas ou erros que podem prejudicar o seu funcionamento. Como tal, deverão ser analisadas as funções críticas e deverão ser criadas soluções de separação de responsabilidades e de verificação de acções.

Exemplo: se um operador insere dados críticos num sistema, deverá existir alguém responsável pela verificação da correcção dos dados inseridos; se existe alguém responsável pela gestão de contas informáticas de administrador, deverá haver alguém que valide acções realizadas.

Segurança Lógica

Sem a existência de medidas de segurança lógica, a informação em suporte digital encontra-se exposta a ataques. Alguns destes ataques são passivos, na medida em que apenas capturam os dados, sem os alterar, enquanto que outros são activos, afectando a infor-

mação com o intuito de a corromper ou destruir. O catálogo de ataques possíveis é por demais volumoso, e a tendência é para piorar: com a crescente introdução de tecnologias baseadas na comunicação directa entre aplicações, na transferência automatizada de estruturas de dados, potencialmente executáveis, o panorama tende a adensar-se.

Esta é, provavelmente, a área mais rica, mais complexa e provavelmente mais difícil de gerir da segurança empresarial. O ritmo a que se sucedem as gerações tecnológicas, bem como a crescente complexidade das mesmas, faz com que qualquer esforço de adaptação e manutenção da actualidade das tecnologias empregues seja, quase sempre, infrutífero. O número alargado de disciplinas abarcadas pela segurança lógica torna a tarefa do responsável pela segurança uma actividade frenética e muitas vezes frustrante.

Três grandes áreas se destacam no campo da segurança, abarcando a totalidade dos temas desta disciplina: prevenção, protecção e reacção. Dentro de cada uma destas áreas encontramos sub-tópicos que deverão ser considerados, alguns dos quais abordaremos de seguida.

Autenticação e Controlo de Acesso

A autenticação e o controlo de acesso são dois aspectos omnipresentes na vida quotidiana. Ao passarmos um cheque, autenticamo-nos por intermédio da nossa assinatura, que deverá ser idêntica à que consta da base de dados do nosso banco. Ao utilizarmos uma caixa ATM, o acesso é controlado por intermédio de um cartão e de um PIN a ele associado. Inconscientemente, impomos estas medidas de controlo no nosso relacionamento diário, quer seja ao atender um telefone, autenticando o interlocutor por intermédio da sua voz, quer seja abrindo a porta de nossa casa, controlando quem pode entrar através da utilização de uma chave.

Nos SI, a autenticação e o controlo de acesso são igualmente importantes. São eles quem assegura que nós somos quem dize-

mos ser e quem nos permite aceder àquilo a que temos direito, quer ao nível da infra-estrutura (redes de comunicações), quer ao nível aplicacional, através do fornecimento de credenciais do nosso conhecimento exclusivo.

A discussão sobre os melhores métodos de autenticação e de controlo de acessos não tem sido pacífica e tem assistido à introdução regular de novos elementos, tais como cartões inteligentes (*smart cards*) ou dispositivos de autenticação biométrica, bem como à evolução de outros, como os sistemas de gestão de palavras-passe.

A grande questão que se coloca neste debate é, fundamentalmente, a de descobrir qual é a melhor forma de autenticar alguém e de garantir que apenas as pessoas autorizadas têm acesso aos recursos disponibilizados.

As palavras-passe são actualmente a norma no que toca à autenticação de qualquer utilizador perante um sistema. Esta solução, baseada em "algo que eu sei", se bem que amplamente implantada, levanta vários problemas, muitos deles de extrema gravidade.

Para começar, a gestão das palavras-passe pode facilmente tornar-se num quebra-cabeças para o utilizador: é necessária uma palavra-passe para aceder ao sistema e/ou à rede, outra para o correio electrónico, outra para a conta de *webmail*, outra para o sistema de *instant messaging*, outra para a consulta da base de dados, outra para outro recurso e por aí adiante. A juntar a estes elementos, ainda temos todos os outros números e códigos de que necessitamos no dia-a-dia, tais como PINs dos vários cartões de débito e/ou crédito que possuímos, os números de telefone que utilizamos com mais frequência, os números de identificação pessoal, etc. É, então, natural que, em grande parte dos casos, os utilizadores optem pela solução mais fácil que, no caso das palavras-passe, poderá ser a utilização da mesma para todos os recursos ou, mais simplesmente, a manutenção de uma lista escrita, à qual muitas vezes não se dá grande importância e que, por isso, é vulnerável.

Do lado dos administradores de sistemas, o panorama não é menos complicado: para além dos pedidos frequentes de ajuda dos utiliza-

dores que se esqueceram da sua palavra-passe, há a questão das decisões estratégicas que possuem forte impacto sobre este mecanismo de autenticação. O nível de complexidade a exigir na criação de palavras-passe ou a validade das mesmas, por exemplo, são questões que têm necessariamente de ser enfrentadas, muitas vezes no dia-a-dia. E as opções tomadas podem afectar negativamente o desempenho diário da organização, criando obstáculos à autenticação, muitas vezes sem a contrapartida de uma maior garantia de segurança.

As palavras-passe são, então, um mal necessário e, por isso mesmo, começa-se a procurar maneiras de as substituir por formas mais simples e mais seguras.

Uma dessas formas é a utilização de cartões inteligentes, ou *smart cards*, solução esta que associa "algo que eu sei" a "algo que eu possuo". Um *smart card* é um cartão com um circuito integrado capaz de armazenar dados de forma segura, tais como certificados digitais ou chaves criptográficas, protegido por um PIN. É esta capacidade que permite, para além da diversificação dos códigos de autenticação (armazenados na memória do cartão), o isolamento destes elementos de segurança, uma vez que a informação não reside nos sistemas. Para além disso, ao utilizar um PIN para proteger os dados que contém, o *smart card* acrescenta mais um nível de segurança relativamente às palavras-passe: de facto, enquanto que uma palavra-passe tem de ser comunicada ao sistema, podendo ser interceptada em trânsito, a utilização de um PIN, associado localmente ao cartão, diminui esse perigo.

Se bem que apresentem alguma resistência a tentativas de violação e/ou de extracção de informação, não são, infelizmente, a solução milagrosa para os problemas da autenticação. Um cartão pode ser perdido, ou roubado, o que levanta sérios problemas – se todos os dados de acesso residirem num cartão, e esse cartão estiver indisponível, o que acontece?

Surge então a biometria. Teoricamente, esta alternativa, ao basear-se em "algo que eu sou", trazia consigo a promessa de tornar vir-

tualmente impossível enganar o sistema. Na prática, as coisas não funcionam tão bem.

Por ser uma tecnologia numa fase ainda um pouco incipiente, a questão dos "falsos-negativos" adquire uma particular importância. Os sistemas existentes no mercado, dos quais se destacam os leitores de impressões digitais pelo seu preço relativamente acessível e nível de implantação, não são ainda suficientemente precisos ao ponto de reconhecer de forma fiável e consistente os utilizadores autorizados. Por outro lado, os leitores de íris ocular e de reconhecimento facial, por serem ainda demasiado dispendiosos, não se constituem como alternativa. Podem ainda surgir situações em que, com a introdução de autenticação biométrica baseada na leitura de impressões digitais, se se verificarem níveis de negação de acesso a utilizadores legítimos bastante elevados, podem surgir níveis de frustração também demasiado elevados.

Para além desta questão mais técnica, há que ponderar os elementos psicológicos associados a esta tecnologia, nomeadamente a potencial falta de aceitação, por parte dos utilizadores, em que uma organização fique com registos das suas características físicas. Aqui convém tornar extremamente claro à comunidade de utilizadores destes sistemas que a informação armazenada se limita a matrizes de coordenadas geométricas, não reversíveis: ou seja, nem a Empresa guarda uma imagem da característica física utilizada para autenticação, nem o registo que é guardado pode alguma vez ser utilizado para reconstruir essa característica.

Com o evoluir da tecnologia e com acções de esclarecimento junto dos utilizadores, as questões acima apresentadas poderiam ser resolvidas. Então, porque é que não se assiste a uma maior implantação de sistemas biométricos?

Por duas ordens de factores. Em primeiro lugar, os custos associados a estas soluções levam a que apenas possam ser consideradas em implementações limitadas, tais como no controlo de acessos a zonas extremamente sensíveis. Por outro lado, existem formas de ludibriar o sistema. Um investigador da universidade japonesa de

Yokohama recolheu impressões digitais, entre outros, em copos de vidro e, através de um processo simples e pouco dispendioso, criou "dedos" de gelatina que, em 80% dos casos, conseguiram enganar os leitores biométricos.

Claro que existem sistemas capazes de detectar "vida" nos objectos que tentam reconhecer. Mas, mais uma vez, os custos associados não permitem considerá-los, em grande parte dos casos, como opção. Porém, e devido ao enorme número de vantagens oferecidas pela biometria, será previsível uma taxa de penetração cada vez maior, à medida que as soluções existentes forem sendo aperfeiçoadas e os custos se tornem mais acessíveis.

Outras tecnologias que tentam retirar o fardo da Administração de um conjunto alargado de elementos de autenticação são o "*single sign-on*" e as infra-estruturas de chaves públicas.

A primeira propõe substituir-se ao utilizador em todos os processos de autenticação, bastando a este fornecer uma única palavra-passe ao sistema. Se bem que existam aplicações capazes de integrar esta tecnologia, ela ainda não é suportada pela grande maioria dos sistemas. Este factor resulta, em muitos casos, num acréscimo desnecessário de complexidade em sistemas heterogéneos, incapazes de comunicar entre si as credenciais dos utilizadores.

A segunda, ao propor uma solução centralizada de gestão de chaves criptográficas públicas e de certificados digitais, tenta alcançar o mesmo objectivo. Contudo, a evolução de soluções baseadas nesta tecnologia tem sido lenta e complexa. A adopção de padrões (*standards*) tecnológicos não é uniforme, o que atrasa a criação de mecanismos homogéneos; por outro lado, a gestão das chaves e dos certificados coloca questões de extrema complexidade, como por exemplo, as de quem autentica quem, quem é responsável pela revogação dos certificados, etc.

Como vimos, a autenticação e o controlo de acessos constituem um "tema quente" da segurança digital e não existe uma resposta simples e unívoca para a questão de qual é a melhor forma de autenticar utilizadores e controlar o acesso aos recursos.

Mais uma vez, esta resposta dependerá das características particulares de cada ambiente e deverá ser ponderada tendo em linha de conta as necessidades e possibilidades específicas das tecnologias empregues pelo negócio. Se as palavras-passe são suficientes para muitos casos, outros haverá em que se justifica a sobreposição de elementos de autenticação: uma palavra-passe e um *smart card*, ou um cartão e um leitor biométrico.

Só depois de uma análise cuidada das necessidades de segurança da organização e do confronto destas com os recursos disponíveis e com a capacidade de integração e gestão de novas tecnologias, é que o responsável pela segurança da Empresa poderá decidir sobre o caminho a seguir.

Criptografia

Para além de todas as medidas "clássicas" de segurança lógica que possam ser utilizadas para a protecção dos dados existentes em suportes digitais, tais como palavras-passe, gestão de privilégios, etc., existe um mecanismo, já antigo mas de visibilidade relativamente reduzida, que permite garantir a confidencialidade dos dados armazenados. Esse mecanismo é a cifra, também designada criptografia (uma adopção literal do termo anglo-saxónico "*cryptography*").

Na sua essência, a cifra é o processo através do qual se protege (encripta) um conjunto de dados, de modo a que este apenas possa ser desprotegido (desencriptado) por alguém que conheça um determinado segredo. Utilizando um algoritmo de cifra e adicionando-lhe uma chave (palavra ou frase secretas), gera-se uma operação matemática de substituição dos dados a proteger por outros elementos.

O algoritmo é tanto mais poderoso (e eficiente) quanto melhor for a utilização que faz dessa chave e quanto mais resistente for à criptoanálise (processo que tenta descobrir o conteúdo cifrado pelo algoritmo, sem necessitar de qualquer chave).

Actualmente existem vários algoritmos e vários modos de utilização dos mesmos. Relativamente aos algoritmos, queremos apenas chamar a atenção para a importância destes não serem "secretos". Existe, no mercado, uma oferta de vários produtos de cifra que recorrem a algoritmos privativos (secretos), desenvolvidos pelas companhias que os comercializam, e cujas especificações não são públicas. Estes produtos costumam normalmente alegar níveis impressionantes de protecção e invulnerabilidade. Contudo, quanto mais "secreto" for o processo, mais o devemos recear. De facto, na cifra, o importante não é o algoritmo em si, mas o modo como funciona e como utiliza a chave, sendo que os algoritmos que se encontram publicados, ou seja, que não são "secretos", já foram sujeitos a intensos esforços de cripto-análise e deram provas da sua robustez (ou ausência dela). Estes são os mais fiáveis e aqueles que devemos considerar sempre que pensemos em utilizar cifra, enquanto que os algoritmos proprietários e não divulgados podem encerrar graves problemas de segurança na protecção dos dados.

Relativamente ao modo como esta solução é utilizada, existem, fundamentalmente, duas possibilidades: "chave secreta" (criptografia simétrica) e "chave pública/chave privada" (criptografia assimétrica).

Enquanto que, no primeiro caso, é utilizada a mesma chave para cifrar e decifrar os dados, no segundo é utilizado um par de chaves. Resumidamente, na criptografia assimétrica, o utilizador cria um par de chaves (pública e privada), associadas entre si. Para cifrar os dados é utilizada a chave pública, que, como o nome indica, pode ser livremente distribuída; para os decifrar, é utilizada a chave privada, que é do exclusivo conhecimento do seu detentor. A vantagem deste último método relativamente ao primeiro é a de que se evita a necessidade de possuir um canal seguro para a transmissão da "chave secreta", bastando somente garantir a segurança da chave privada. Através da distribuição da chave pública, qualquer remetente pode cifrar dados com essa chave, tendo a garantia de que apenas o detentor da correspondente chave privada terá acesso aos mesmos. Adicionalmente, o possuidor da chave privada

pode utilizá-la para cifrar dados (que poderão ser decifrados com a sua chave pública), conseguindo desta forma comprovar a origem desses mesmos dados: a decifragem de dados com a chave pública de alguém implica obrigatoriamente que eles tenham sido cifrados com a chave privada correspondente[8].

Existem igualmente soluções que utilizam ambas as técnicas: a criptografia assimétrica é usada para o estabelecimento da comunicação segura inicial e para a troca de uma chave simétrica, que será utilizada na restante comunicação. A vantagem desta solução reside na diminuição da carga computacional, uma vez que a criptografia assimétrica requer um maior esforço computacional relativamente à criptografia de chave simétrica, ganhando-se assim em termos de desempenho.

Relativamente aos algoritmos mais conhecidos e utilizados, gostaríamos de abordar apenas dois, devido à sua enorme popularidade, importância e presença no mercado: o DES e o AES.

O DES (*Data Encryption Standard*) foi adoptado pelo governo norte-americano, em 1981, como o *standard* para a protecção de informação electrónica. Como consequência, a sua utilização foi amplamente adoptada por vários sectores da sociedade, americana e não só. Depois de sucessivas revisões do algoritmo, tentou-se obter um nível superior de protecção e, em 1999, surgiu o TripleDES (ou 3DES) como evolução do *standard*. O funcionamento deste último algoritmo é, de um modo simples, composto por três operações sequenciais de cifra utilizando o DES, o que proporcionou um nível de segurança bastante superior.

Em 1997, a agência de normas americana lançou um concurso público para a criação de um algoritmo mais robusto. Após uma exaustiva análise dos vários concorrentes, a 26 de Maio de 2002 entrou em vigor um novo *standard* de cifra: o AES, ou *Advanced*

---

[8] De notar que é não possível decifrar, com a chave pública, informação cifrada com essa mesma chave.

Encryption Standard, baseado num algoritmo chamado Rijndael. Este é, actualmente, o algoritmo obrigatório, nos Estados Unidos, para as operações governamentais e para algumas civis (por exemplo, nos mercados financeiros).

Devido à recente adopção deste *standard*, o seu suporte ao nível aplicacional ainda não é abrangente e não se prevê que o venha a ser no curto prazo.

Perante o exposto, ao considerar a possibilidade de adquirir uma solução de cifra, a Empresa deverá obter informações sobre a robustez do algoritmo utilizado, bem como sobre a possibilidade de migração para algoritmos mais evoluídos e robustos, como sejam o AES. Porém, as soluções que utilizem o 3DES ainda podem ser consideradas, atendendo a que este é um dos algoritmos mais fortes no mercado.

IPv6

O IPv6 (*Internet Protocol version 6*) ou IPng (*Next Generation Internet Protocol*) encontra-se em fase de desenvolvimento, existindo já suporte aplicacional para esta nova versão do protocolo que suporta a Internet. O seu surgimento deve-se, em grande medida, à necessidade de criação de um novo esquema de atribuição de endereços, uma vez que o "espaço de endereçamento" (*address space*) oferecido pelo IPv4 – actualmente em utilização – se encontra quase esgotado, tornando-se cada vez mais difícil, devido à sua escassez, a obtenção de endereços públicos ("oficiais") para ligação de novos sistemas à Internet.

Se bem que tenha sido esse o principal impulsionador para o desenvolvimento desta nova versão da tecnologia, os grupos de trabalho envolvidos aproveitaram a ocasião para aperfeiçoar o protocolo, introduzindo, entre outras, capacidades de regulação da qualidade de serviço e de autenticação e privacidade. Assim, o IPv6 inclui a definição de extensões que suportam as necessidades de autenticação, integridade e confidencialidade das comunicações, ao

nível do protocolo (i.e., no nível que suporta as aplicações), podendo ser utilizados vários algoritmos – o algoritmo proposto é o DES (*Data Encryption Standard*).

À medida que este protocolo se torne mais comum, através da sua adopção por parte dos utilizadores, ficará disponível mais um mecanismo de protecção de dados.

Infra-Estrutura de Chaves Públicas

Na criptografia assimétrica apenas é necessária a chave pública do destinatário para cifrar dados destinados exclusivamente a esse destinatário. No entanto, à partida, não há quaisquer garantias de que a chave conhecida é, de facto, a do destinatário pretendido.

Um tipo de ataques assente nesta vulnerabilidade envolve um terceiro elemento, capaz de interceptar as comunicações entre duas partes (designado de "ataque de homem no meio" – "*man-in-the-middle attack"*). Supondo que X quer enviar a Y informação confidencial, utilizando criptografia assimétrica, irá solicitar a Y o envio da sua chave pública para cifrar os dados. Se esse pedido for interceptado por Z, este poderá enviar a X uma falsa chave pública, alegadamente pertencente a Y. X irá então utilizar essa chave para cifrar a informação e enviá-la-á a Y. Contudo, Z tornará a interceptar a comunicação, decifrará os dados com a chave falsa e, utilizando a chave legítima de Y, tornará a cifrá-los para os enviar para este último. As comunicações entre X e Y são, assim, do pleno conhecimento de Z, sem que X e Y disso tenham qualquer consciência (ver Fig. III-1).

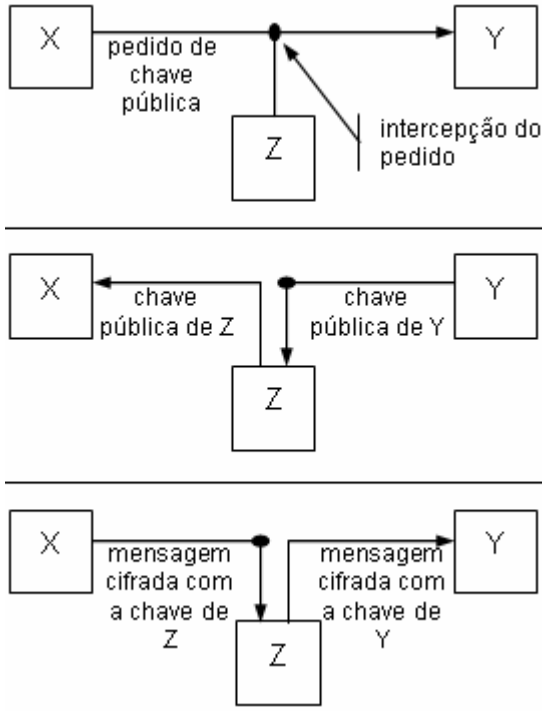


Fig. III-1: Ataque *man-in-the-middle*

A infra-estrutura de chaves públicas, ou PKI (*Public Key Infrastructure*), é a combinação de software, cifra e serviços que permitem a protecção e autenticação de comunicações digitais, através da gestão segura de chaves criptográficas. Esta tecnologia integra certificados digitais, criptografia de chaves públicas e autoridades de certificação numa arquitectura de segurança abrangente, introduzindo um elemento de garantia na criptografia assimétrica.

Ao utilizar uma solução PKI, associando certificados às chaves criptográficas, este ataque não será possível, uma vez que o que Y enviaria a X não seria apenas a sua chave pública, mas um certificado contendo, para além da sua chave criptográfica, informação inequivocamente ligada à sua identidade, o que permitiria a X validar a informação recebida junto de um terceiro elemento: a Autoridade Certificadora.

Uma solução PKI depende das Autoridades Certificadoras (*Certification Authorities*), ou CA. Esta é a unidade fundamental de qualquer infra-estrutura deste tipo, uma vez que é a única detentora do poder de emissão e revogação de certificados de chaves públicas. Estes certificados são assinados digitalmente pela CA e, deste modo, associam indelevelmente a chave emitida ao seu detentor.

Quando um utilizador final pretende obter um certificado de chave pública (gerada em simultâneo com a chave privada), tem de se registar junto da CA que requer, para tal, comprovativos oficiais. Este processo pode ser realizado directa ou indirectamente, através de intermediários, de acordo com as exigências da certificação em causa. Uma vez registado, o utilizador recebe informação exclusiva que, autenticando-o inequivocamente, lhe permitirá continuar o processo. O processo continua com a criação de um par de chaves (pública/privada), podendo esta acontecer no momento do registo ou como consequência deste. Finalmente, o utilizador faz um pedido formal de um certificado digital que, nesta fase de certificação, associa ao seu par de chaves criptográficas a informação requerida pela CA (de identificação do utilizador).

No final deste processo, o utilizador passa a deter um instrumento de autenticação garantido e não repudiável (na medida em que constitui uma prova inegável de uma acção), bem como uma forma certificada de protecção de dados.

A CA, núcleo central de todo este processo, pode ser uma entidade oficial[9], de conhecimento público, ou poderá ser simplesmente uma componente da Empresa, no caso de se implementar uma solução PKI interna. Com estes certificados, e com a integração desta tecnologia nos sistemas informáticos, a autenticação e verificação de utilizadores é grandemente facilitada. Para além disso, em transacções formais, entre empresas, os certificados digitais oficiais (ou

[9] Em Portugal, a autoridade credenciadora de entidades certificadoras é o Instituto das Tecnologias da Informação na Justiça, assistido pelo Conselho Técnico de Credenciação.

seja, emitidos por uma CA reconhecida) possuem a validade de assinaturas e são suficientes para firmar transacções.

Uma questão pertinente no que toca aos certificados digitais prende-se com a sua validade. De facto, estes possuem uma validade definida, após a qual deixam de poder ser utilizados. Adicionalmente, quando uma chave é comprometida, torna-se necessário proceder à sua invalidação, ou seja, revogar a chave. Compete à CA emitir listas de certificados inválidos e divulgar ou disponibilizar essas listas a toda a comunidade de utilizadores. Esta tarefa, como se depreenderá facilmente, corre o risco de assumir proporções avultadas, pelo que pode constituir um problema de gestão acrescentado.

Para além desta questão relacionada com a gestão, existe ainda o tema da segurança e da confiança: se a CA constitui o núcleo central de todo o processo, é necessário que exista um grau de confiança absoluto nesta entidade, pois os certificados por ela emitidos obrigam os seus detentores. A questão que se coloca é, então, a de quem certifica a CA. No caso de existir uma autoridade formal, oficial, essa questão não será muito pertinente, mas nos casos em que não exista, até que ponto se pode realmente confiar nos certificados emitidos por esta ou por aquela CA comercial ou empresarial?

Por outro lado, no processo de registo e emissão do certificado, quais são as medidas tomadas pela CA para verificar a identidade de quem solicita o certificado? Podem revestir-se de grande formalidade com, por exemplo, assinaturas presenciais, mas poderá ser muito mais simples. Em Janeiro de 2001, e devido a uma falha humana no processo de verificação de identidade, a Empresa VeriSign, responsável pela emissão de certificados digitais, emitiu dois certificados a alguém que se apresentou como representante da Microsoft[10]. Como consequência, esse atacante passou a deter um

[10] Cert Advisory CA-2001, “Unauthentic «Microsoft Corporation» Certificates, 22 de Março de 2001.

instrumento que lhe permitiria, entre outros, assinar código como sendo produzido pela Microsoft, enganando potencialmente os destinatários desse software e levando-os a confiar em algo que não era o que afirmava ser.

Em suma, uma solução PKI envolve pormenores que podem causar falhas do sistema se não forem devidamente verificados e implica uma carga de gestão que pode assumir proporções indesejadas. Contudo, para algumas necessidades (como, por exemplo, para o relacionamento com fornecedores ou parceiros), a PKI pode constituir uma solução viável, e mesmo, a nível interno, em organizações de grande dimensão, pode representar uma enorme mais-valia no que diz respeito ao correio-electrónico.

Kerberos

Kerberos é um protocolo de autenticação de rede, desenvolvido pelo Massachussetts Institute of Technology (MIT), que utiliza criptografia forte, partindo do princípio de que todas as transacções entre clientes e servidores se irão realizar em redes não seguras.

O princípio deste protocolo é bastantes simples: sempre que um cliente deseja aceder a recursos disponíveis na rede, autentica-se junto de um servidor seguro, designado Kerberos, que constitui o Centro de Distribuição de Chaves (*Key Distribution Center*) para a rede. Uma vez autenticado, o cliente recebe um "bilhete" (*ticket*) do servidor, que lhe permitirá autenticar-se criptograficamente junto dos detentores dos recursos a que pretende aceder, garantindo desta forma ser quem é e estabelecendo um canal de comunicações seguro.

Os problemas com este protocolo residem nas diferentes formas de implementação. Estas são influenciadas pela topologia de rede, pelos protocolos utilizados para a autenticação (por exemplo, um servidor POP [*Post Office Protocol*] que valide uma palavra-passe junto de um servidor Kerberos não é seguro) e pelo tipo de integra-

ção do protocolo de autenticação de rede por parte da aplicação que afirme suportá-lo.

Por outro lado, a implementação deste mecanismo feita pela Microsoft, que o integra nos seus sistemas operativos mais recentes, levanta questões ao nível da conformidade com o standard definido. Se num ambiente puramente Microsoft este factor não é problemático, quando se pretendem criar interacções com outros sistemas (Unix, por exemplo), é necessário um esforço considerável de integração e de mediação.

Independentemente destas questões, o Kerberos afigura-se como uma possibilidade a ter em conta para transacções seguras, em ambientes controlados (ou seja, sob o controlo exclusivo da organização) e, precisamente devido à sua integração com os sistemas operativos (SOs) da Microsoft, poderá ser uma opção viável para quem utilize exclusivamente estes SOs.

VPN

As redes privadas virtuais, ou *Virtual Private Networks* (VPN), assentam em tecnologias que, através da utilização de vários protocolos e medidas de segurança, criam canais seguros de comunicação em ambientes públicos, como a Internet. Todos os dados transmitidos através destes canais, ou "túneis", são cifrados e possuem controlo de integridade, o que significa que, caso sejam alterados em trânsito, são rejeitados pelo destinatário e retransmitidos pelo emissor.

O protocolo mais amplamente utilizado nesta tecnologia é o IPSec, embora existam outros.

O IPSec (*IP Security*) é o standard utilizado na Internet para a criação de túneis, para encriptação e para autenticação. A protecção do tráfego é conseguida através da resolução, na fase de concepção do protocolo, de questões como:

- controlo de acessos;

- integridade da ligação;
- autenticação da origem dos dados;
- protecção contra a reprodução dos dados;
- confidencialidade do fluxo de tráfego.

Para a criação de comunicações seguras, na Internet, a comunicação entre um cliente e um servidor por exemplo é, então, estabelecida com recurso ao protocolo IPSec, sendo os dados cifrados e encapsulados dentro dos pacotes IP. Para o estabelecimento deste túnel, é necessário que ambas as partes se reconheçam mutuamente, para o que, depois de um contacto inicial, os intervenientes na comunicação acordam numa chave criptográfica que será utilizada para cifrar o restante conteúdo da interacção.

Uma vez determinada a chave, todos os dados posteriores serão cifrados e transmitidos através da infra-estrutura pública, sem que possam, mesmo que capturados, ser entendidos por quaisquer intermediários.

Esta solução oferece vantagens económicas óbvias relativamente às linhas dedicadas, directas, uma vez que utiliza a infra-estrutura pública para transacções privadas. Apesar de ainda existirem algumas questões relativamente aos *standards* aplicáveis, nomeadamente ao protocolo IPSec, esta tecnologia, pela sua conveniência, foi largamente adoptada pela comunidade, suportando actualmente comunicações em todas as áreas de actividade.

A implementação desta solução implica a existência, em todos os sistemas que devam comunicar entre si, de tecnologia VPN, ou seja, software e/ou hardware que permita autenticar os interlocutores e cifrar as transacções. Outro dos requisitos das VPN é o de que esta deve ser perfeitamente definida, significando que apenas o administrador da rede segura tem a capacidade de adicionar ou remover participantes. Estes requisitos significam um esforço de configuração que pode ser bastante avultado, dependendo do número de interlocutores. Para além desta configuração inicial, a definição e aplicação de políticas de segurança (quem pode aceder

a quê, como e quando) é um factor a ter em conta. A simples adição de um novo nó a uma VPN já existente poderá implicar a configuração individual de todos os nós, para que sejam possíveis comunicações bidireccionais entre si – este facto poderá não ser grave numa rede pequena mas, numa rede com, por exemplo, 100 nós, equivale a 200 alterações nas políticas existentes.

As políticas de segurança da VPN definem basicamente os diferentes privilégios de acesso. Estes podem ser configurados de acordo com as necessidades dos utilizadores, sendo que as políticas deverão ser suficientemente granulares para permitir a diferenciação de acordo com as diferentes necessidades, níveis de confiança, etc. Compete, então, ao administrador da VPN a criação e manutenção de regras que sejam suficientemente seguras em termos de controlo de acesso à informação, mas que não se tornem impeditivas da produtividade.

Um outro aspecto a ter em linha de conta é o de que, por se tratarem de dados cifrados, estes não serem verificáveis nos pontos de entrada, por exemplo, pelas *firewalls* existentes, podendo deste modo originar a passagem de conteúdos proibidos ou de código malicioso através dos mecanismos de protecção implementados no perímetro da rede interna.

Para a escolha da solução de VPN a implementar, o responsável pela segurança deverá, por fim, considerar os seguintes pontos:

- Que tipo de clientes vão existir na VPN: somente clientes internos (da Empresa), ou também externos (parceiros, clientes, etc.)? Esta decisão pode ter impacto sobre o tipo de tecnologia a seleccionar, podendo ser preferível optar por uma solução que não implique grandes esforços de configuração dos clientes.
- Que tipo de gestão é oferecida pelo produto? Dependendo das circunstâncias, poderá ser suficiente uma gestão descentralizada mas, no caso de implementações volumosas, a escolha deverá recair sobre uma plataforma de gestão centralizada.

- Que tipo de autenticação é oferecido? Existem várias hipóteses, desde nome de utilizador/palavra-passe, certificados ou palavras-passe de utilização única (*one time password*). A potencial complexidade de gestão destes elementos é um ponto a considerar na escolha.
- Que tipo de algoritmo criptográfico é suportado pelo protocolo da VPN? Relativamente a este componente, há que optar pela robustez e eficácia comprovadas (TripleDES ou AES), considerando a compatibilidade com os nossos parceiros.
- Qual a capacidade de integração na infra-estrutura existente? A VPN deverá poder ser integrada nas soluções já utilizadas pela Empresa como, por exemplo, PKI.

Considerando os elementos atrás expostos, a Empresa deverá, ainda, equacionar a eventual criação e manutenção de VPNs de acordo com as aplicações que pretende ver suportadas. Caso estas sejam fundamentalmente baseadas em tecnologia Web, a possibilidade de criação de soluções baseadas em SSL (*Secure Sockets Layer*) pode ser uma alternativa. Contudo, dever-se-ão respeitar as recomendações de segurança dos produtores do software SSL, uma vez que este, se não for devidamente configurado e actualizado, pode padecer de alguns problemas de segurança.

Antivírus

Actualmente, poucas são as organizações que não utilizam, de forma mais ou menos coordenada, qualquer mecanismo antivírus nos seus sistemas. De facto, com a actual proliferação de código malicioso e de ferramentas destinadas a criar vírus, é quase "suicídio" criar uma ligação entre dois sistemas sem pensar em qualquer tipo de protecção contra estas ameaças.

As aplicações existentes para a detecção de vírus baseiam-se em assinaturas para cumprir a sua função. Uma assinatura mais não é

do que um excerto do código binário único de um vírus, que permite a identificação do vírus em questão por um simples processo de comparação.

Estas soluções obrigam à permanente actualização das bases de dados de assinaturas (e, com menos frequência, dos motores de detecção e de remoção), bem como à disseminação dessas actualizações por todos os sistemas a proteger. A consequência, caso não exista um cuidadoso planeamento prévio, pode ser um enorme esforço de actualização dos produtos antivírus existentes que, ao ritmo de aparecimento de novos vírus, pode tornar-se uma batalha perdida.

Felizmente, existem soluções centralizadas que permitem realizar automaticamente todas estas tarefas a partir de um único ponto. Para as seleccionar, o responsável pela segurança deverá avaliar as características de cada uma, bem como as necessidades da Empresa, devendo ter em conta os seguintes aspectos:

- Qual o grau de facilidade na obtenção de actualizações da base de dados de assinaturas? Este processo deverá ser simples, automático e não deve causar quaisquer problemas ao administrador.
- Qual o grau de facilidade na disseminação das actualizações pelos clientes? O processo deverá ser o mais escorreito e fiável possível.
- Qual o tempo de resposta do produtor do antivírus a vírus novos? Esta resposta nunca deverá exceder algumas horas.
- Que possibilidades existem para a gestão dos clientes:
  - podem ser agrupados em tipos de utilizadores?
  - podem ser criados grupos prioritários para a actualização?
- Que possibilidades existem para a gestão do antivírus:
  - As regras podem ser definidas centralmente?

- Podem ser impedidas alterações locais?

- Que tipo de alertas e de relatórios são produzidos? Os relatórios devem indicar as actualizações de versões, as detecções de vírus e as acções realizadas.

- Como é o suporte técnico do fabricante? Muitas destas soluções, se bem que de utilização simples, podem ser complexas de instalar e configurar. O apoio técnico revela a sua importância na capacidade de auxílio na resolução dos problemas mais simples.

Para além das soluções antivirais baseadas em assinaturas, começam a surgir outras, mais actuais, baseadas em comportamentos.

Uma solução antivírus baseada no comportamento não procura características binárias identificativas de código malicioso, mas antes analisa o modo como o software interage com o sistema. Se um qualquer programa tentar aceder à lista de endereços de correio electrónico, por exemplo, esse poderá ser um sinal de infecção viral. A lógica de funcionamento destas soluções inspira-se na detecção de intrusões e promete um nível superior de eficácia na detecção e contenção de infecções.

Porém, esta tecnologia encontra-se numa fase ainda incipiente, pelo que a sua adopção deverá ser gradual e progressiva.

Em resumo, independentemente da tecnologia utilizada, não se deve descurar a actualização e acompanhamento constante deste tipo de soluções, especialmente nos sistemas informáticos com ligações a outras redes de comunicações, e muito particularmente nos servidores de correio-electrónico.

A detecção de vírus é, em suma, uma necessidade imperiosa de qualquer organização.

Filtragem de Conteúdos

Um outro aspecto da segurança lógica, que se pode relacionar com a detecção de vírus, é o da filtragem de conteúdos. De facto, a filtragem de conteúdos está para o corpo das mensagens de correio electrónico ou para os conteúdos *web* como o antivírus está para os anexos do *e-mail*. Efectivamente, muitas das soluções de antivírus existentes utilizam, inclusivamente, uma qualquer espécie de filtragem, bloqueando o acesso a conteúdos potencialmente nocivos. Mas este tipo de protecção não se esgota no evitar de infecções virais.

Para além disso, estas soluções podem evitar outro tipo de quebras de segurança. Se, por exemplo, for utilizado um mecanismo de filtragem de conteúdos no servidor de correio-electrónico da organização, este poderá detectar tentativas, voluntárias ou não, de transmissão de informação confidencial. No caso da Empresa optar por uma solução deste tipo, deverá certificar-se de que os seus colaboradores têm conhecimento da sua existência, pois estará a negar-lhes o direito à privacidade.

Existe igualmente a possibilidade de bloquear o acesso a determinados sítios na Internet com base em listas de endereços (URL), definidas pelo fornecedor da solução de filtragem e aperfeiçoadas pela Empresa, ou com base em palavras-chave relacionadas com quaisquer temáticas que se pretendam bloquear. Estas soluções podem eliminar uma parte considerável das visitas a conteúdos pornográficos, a repositórios de *software* “pirata”, a filmes copiados ilegalmente, etc.

Em termos de produtividade, estas ferramentas de filtragem podem produzir resultados imediatos. Ao permitir definir, no ponto de acesso à Internet, quais os conteúdos que não são admitidos na Empresa (como, por exemplo, ficheiros de som, determinado formato de imagens, etc.), uma solução de filtragem pode economizar os recursos existentes, evitando o seu consumo em actividades não relacionadas com o negócio, quer se trate do intercâmbio de “con-

teúdos proibidos" por correio, quer da consulta a sítios na Internet com informação de utilidade "duvidosa".

Redundância

Já no campo da protecção, a redundância surge como a forma mais óbvia de evitar a indisponibilidade da informação.

Tal como guardamos duplicados das chaves das portas de nossa casa, para o caso de perdermos o original, existem mecanismos, de complexidade variável, que permitem criar duplicados da informação contida nos sistemas informáticos.

A redundância pode ser obtida de várias formas, quer através de cópias manuais de dados, quer através de sistemas automatizados de protecção da informação. Na sua expressão mais complexa, estes mecanismos de protecção podem assumir a duplicação total da infra-estrutura informática existente, numa localização remota, com transferência automatizada de dados entre locais. Este tipo de soluções, normalmente adoptados para estruturas extremamente críticas e sem qualquer tolerância de *downtime*, implica um investimento inicial avultado e custos de manutenção que podem ser igualmente elevados.

Por este motivo, as soluções mais comuns passam pela criação de *clusters* de máquinas e pela implementação de soluções de RAID (*Redundant Array of Inexpensive Disks)* com paridade (em que a informação é partilhada por vários discos, sendo que a indisponibilidade de um deles não implica a indisponibilidade dos dados nele contidos). Em qualquer dos casos, a solução a adoptar deverá ter em conta o valor da informação a proteger. No caso de conteúdos estáticos, pouco actualizados e de valor referencial, bastará talvez a criação e manutenção de cópias de segurança. No caso de bases de dados dinâmicas, com actualizações e consultas muito frequentes, talvez se justifique equacionar a criação de um *cluster*, ou de um sistema de armazenamento centralizado, com duplicação.

Ao nível da infra-estrutura de suporte aos dados, existe a possibilidade de criar soluções redundantes a praticamente todos os níveis. Para além dos *clusters* de máquinas, já referidos, os próprios equipamentos activos da rede de dados (*router*, *switch*, *hub*, etc.) podem ser duplicados, criando estruturas redundantes, como se ilustra no exemplo da Fig. III-2:

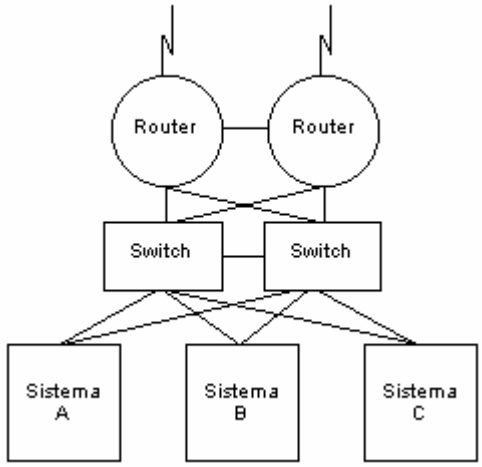


Fig. III-2: Infra-estrutura redundante - Exemplo

A protecção através da redundância encontra-se intimamente ligada com a questão do armazenamento, que será abordada de seguida.

Armazenamento

De uma época em que a capacidade de armazenamento se concentrava num volumoso *mainframe*, passámos para uma fase em que se assistiu à acelerada descentralização de plataformas (e respectivos suportes de dados) e estamos, cada vez mais, a contemplar um cenário de reconcentração da informação, desta feita traduzido em redes dedicadas ao armazenamento, acompanhado pela crescente descentralização do acesso aos mesmos.

A realidade certamente mais preponderante é, no entanto, um misto destas várias tendências: mantém-se o *mainframe*, pelas suas

características e capacidade, gerem-se servidores aplicacionais dispersos, pela sua adaptabilidade, e começa-se a assistir com frequência à introdução de *network attached storage* ou de *storage area networks*, como meio de optimizar investimentos e facilitar a gestão.

As estratégias de protecção da organização, perante esta realidade compósita e frequentemente difícil de abarcar em toda a sua complexidade, detêm-se muitas vezes perante a difícil tarefa de detectar todas as possibilidades existentes. Destaquemos algumas das tendências mais comuns.

Network Attached Storage (NAS) é a forma mais simples e eficiente de adicionar capacidade de armazenamento a uma rede. É composta por sistemas de hardware, dedicados, com capacidade nativa de armazenamento e de ligação à rede informática da empresa. A sua capacidade difere, existindo actualmente fabricantes que afirmam estar perto de conseguir passar a marca do Petabyte em equipamento NAS. Para além de uma instalação simples, a NAS oferece facilidade de gestão, abrangência de clientes heterogéneos, capacidade de crescimento e alguma segurança. Porém, longe de serem o Santo Graal do armazenamento, as NAS levantam algumas questões que deverão ser ponderadas, tais como a inexistência de capacidade nativa para a salvaguarda (*backup*) de dados (o que poderá implicar um acréscimo de tráfego na rede) e, por outro lado, a ausência de mecanismos próprios que protejam os dados da NAS em trânsito durante as cópias de segurança.

A *Storage Area Network* (SAN) é uma rede dedicada ao armazenamento de dados, tendo como principal vantagem a remoção de parte do tráfego que normalmente passaria pela LAN, concentrando-o numa infra-estrutura dedicada de elevado desempenho, podendo ser partilhada pelas mais variadas plataformas e sistemas operativos. Uma SAN é composta por hardware com capacidade de armazenamento (e de crescimento) ligado, por intermédio de fibra (*fibre channels*), à rede da organização.

Se bem que tenha uma aceitação bastante significativa junto do mercado, principalmente devido às suas características de segurança e alta velocidade, esta tecnologia, também não trouxe solução para os problemas associados ao armazenamento: por enquanto, ainda não existem *standards* tecnológicos comuns, adoptados pelos fabricantes, que permitam encarar as SAN com facilidade. A falta destes padrões comuns torna a opção por estas soluções em potenciais investimentos avultados em plataformas de gestão, bem como poderá implicar dependência tecnológica relativa a um fabricante, retirando ao cliente liberdade de escolha. Por outro lado, assiste-se actualmente ao desenvolvimento acelerado de tecnologias de rede, tais como velocidades de 10 Gbps (sobre Ethernet), que farão forte concorrência às velocidades do *fibre channel* e às conveniências das SAN.

Perante a diversidade e eventual dispersão de suportes de armazenamento, a Virtualização do Armazenamento surge como tentativa de utilizar eficazmente os recursos disponíveis, permitindo a sua gestão centralizada. Este conceito materializa-se em software que cria uma camada de abstracção entre os dispositivos físicos de armazenamento e os sistemas operativos dos servidores, o que significa que os diversos suportes de dados ligados à rede podem ser geridos como se de um único sistema se tratassem (quer sejam sub-sistemas discretos de armazenamento, NAS ou SAN). Ainda que se encontre a dar os primeiros passos, aguardando o impulso do iSCSI (encapsulamento de comandos SCSI em pacotes IP) para dar um grande salto, esta virtualização permite já fazer a gestão da capacidade de armazenamento existente em toda a organização a partir de um único ponto central. As características desta solução, incluindo ajustes automáticos do espaço disponível, notificações e a possibilidade de gestão de espaço através de estatísticas de metadados, são aliciantes. Porém, ao permitir a gestão de vários suportes de armazenamento como se de um único se tratassem, a virtualização potencia os problemas em caso de desastre, pois a recuperação terá, obrigatoriamente, de incluir todos os sistemas

pertencentes ao esquema de armazenamento virtual e não apenas aqueles verdadeiramente críticos.

Todas as soluções de armazenamento de dados existentes possuem os seus prós e contras. Todas elas dependem, em última instância, das finalidades que visam servir, ou seja, dos objectivos do negócio, pelo que deverão ser cuidadosamente seleccionadas. Compete ao responsável pela segurança o aconselhamento na fase de selecção, para que, posteriormente, a tarefa de protecção das soluções de armazenamento seja conseguida com o menor esforço possível.

Um aspecto intimamente ligado com os dois temas que acabámos de abordar, redundância e armazenamento, é o da recuperação de desastres e continuidade de negócio, abordada no capítulo "Segurança Face ao Desastre".

Salvaguarda da Informação

Já afirmámos mais do que uma vez, neste livro, que a informação é possivelmente o bem mais precioso das empresas, afirmação que, à partida, deverá reunir o consenso de todos. É por existir esta consciência da importância da informação, cada vez dependente de suportes electrónicos, que praticamente todas as organizações possuem um qualquer esquema de salvaguarda dos seus dados mais valiosos.

À medida que aumenta a capacidade de armazenamento disponível e cresce a complexidade dos sistemas de processamento de informação, o volume de dados armazenados segue esta tendência, atingindo proporções significativas. As empresas, cada vez mais, deparam-se com a necessidade de protecção de um conjunto complexo de informação, disperso por vários suportes e gerado por diferentes aplicações. Felizmente, as soluções de salvaguarda, ou *backup*, actuais acompanharam esta evolução e oferecem hoje níveis de desempenho e de protecção amplamente satisfatórios.

A solução mais simples, e por isso mais comum, para criar cópias de segurança da informação consiste na utilização de unidades de *backup*, instaladas nos sistemas ou autónomas, que realizam automaticamente todas as tarefas necessárias à cópia dos dados para tapes, ou fitas magnéticas de armazenamento. Devido ao seu incomparável grau de penetração no mercado, estas soluções há muito que deixaram de ser lineares, passando a oferecer uma ampla gama de possibilidades. Desde as simples unidades individuais de *tapes* com capacidade para algumas dezenas de Gigabytes, passando por sistemas de *backup* com capacidade para algumas centenas de Gigabytes, até bibliotecas de *tapes* robotizadas, complexas e autónomas, podendo albergar vários Terabytes, a oferta existente suprirá, certamente, as necessidades mais diversas, oferecendo a solução para vários problemas a vários níveis.

Recentemente começaram a verificar-se algumas evoluções tecnológicas, dignas de referência, e que se prendem com a capacidade individual de cada tape:

- Super DLT (Digital Linear Tape): esta é a nova geração da plataforma DLT, que pode ser considerada a norma do mercado devido à sua antiguidade. Baseando-se na experiência de vários anos, adquirida no desenvolvimento deste tipo de produtos de cópia de segurança, os fabricantes aumentaram a capacidade destas *tapes* que, actualmente, atinge os 110 GB (sem compressão). Sendo uma evolução da DLT, a Super SDLT garante retrocompatibilidade com as gerações anteriores.

- LTO (*Linear Tape Open technology*): Tecnologia resultante de um consórcio de várias marcas, caracteriza-se pelo facto de ser um formato tecnológico “aberto” que visa permitir o desenvolvimento de ofertas nesta área por parte de vários fabricantes que adiram ao padrão. Os produtos baseados na tecnologia LTO são designados Ultrium e encontram-se actualmente na sua segunda geração (de um total de quatro gerações previstas). A capacidade dos suportes de

segunda geração é de 200 GB por *tape* (sem compressão), visando a meta de 800 GB na última geração. É um corte com a tecnologia DLT.

A opção por uma destas duas possibilidades nem sempre é pacífica, existindo defensores e detractores de ambas. A selecção deverá tomar em conta a infra-estrutura já existente, a necessidade de retrocompatibilidade, a capacidade de armazenamento pretendida a médio/longo prazo e o tipo de suporte oferecido pelo fabricante.

Independentemente da capacidade dos suportes e sistemas, e da complexidade das soluções de *backup* adoptadas, um ponto que deverá ser observado por todas as organizações tem a ver com a gestão diária dos suportes de *backup*.

Uma das primeiras questões a considerar tem a ver com o local onde são armazenadas as cópias de segurança. É óbvio que a colocação de *tapes* na mesma sala onde se encontram os sistemas cujos dados elas protegem não é uma atitude muito inteligente. Dependo da duração pretendida do prazo de retenção (que abordaremos de seguida), as cópias de segurança podem ser armazenadas no mesmo edifício (*on-site*), num piso diferente e protegidas por cofres ignífugos, podem ser transferidas para outro edifício da organização ou podem ser armazenadas por prestadores de serviços (*off-site*).

A rotação destes suportes é, igualmente, um factor de extrema importância para a implementação de um esquema de salvaguarda eficaz. Deve existir um plano de entregas e de recolhas ajustado às necessidades da Empresa e ao esquema de retenção adoptado. Durante o trajecto dos suportes de *backup*, estes devem ser devidamente protegidos contra todas as eventualidades: acidentes, furto, entre outras. Caso se opte pela contratação dos serviços de armazenamento de terceiros, o contrato deverá especificar claramente o calendário de recolha e devolução dos suportes, bem como o prazo máximo de resposta em caso de emergência, i. e., sempre que a Empresa necessitar de recuperar dados perdidos.

Regra geral, os esquemas de *backup* mais comuns enquadram-se na clássica definição de três ciclos: Avô, Pai e Filho. O que diferencia estas três "gerações" de *backups* é, precisamente, a duração do seu prazo de retenção e, eventualmente, o seu local de armazenamento. A cópia de segurança da geração "avô" é tipicamente a que mais tempo é retida, enquanto que o "filho" constitui, normalmente, um *backup* de rotação rápida.

Exemplo:
- Cópia de segurança "avô": *backup* completo dos sistemas, realizado na última sexta-feira de cada mês e retido durante trinta dias (ou mais).
- Cópia de segurança "pai": *backup* completo dos sistemas, realizado todas as sextas-feiras, e retido durante quinze dias.
- Cópia de segurança "filho": *backup* completo de todos os sistemas, realizado diariamente, e retido durante sete dias.

Dependendo do prazo de retenção das cópias de segurança, deverá, então, ser delineado um esquema de armazenamento *on-site* e *off-site*, como forma de garantir a segurança e disponibilidade dos suportes. Nos casos em que exista um grande número de suportes, com prazos de retenção diferenciados, e vários locais remotos de armazenamento, a gestão da rotatividade dos *backups* pode ser complexa.

É para solucionar esta questão que foi desenvolvida uma tecnologia conhecida como *vaulting* electrónico, que consiste simplesmente na ligação das instalações da Empresa a um local remoto, com bibliotecas de *backups* de elevada capacidade, através de linhas dedicadas, preferencialmente de alto débito. Esta solução retira grande parte da complexidade à gestão do armazenamento local e remoto dos suportes de *backup*, uma vez que as cópias de segurança são realizadas directamente nos locais onde ficarão guardadas.

Dependendo dos requisitos de disponibilidade dos dados, a organização poderá sentir a necessidade de possuir uma solução que,

mais do que criar cópias de segurança, garanta a duplicação em tempo quase real dos dados processados. Nestes casos, a complexidade e custo da infra-estrutura necessária aumenta, oferecendo em contrapartida um maior grau de fiabilidade na protecção da informação.

Neste campo o *mirroring* pode ser considerado como a possibilidade mais simples e mais económica. Consiste na duplicação do espaço de armazenamento, utilizando controladores específicos que escrevem (quase) simultaneamente em dois suportes, um primário (o de produção) e um secundário (de *backup*). Este conceito não é mais do que a expansão das estratégias de protecção de dados existentes ao nível dos discos rígidos, com a grande diferença de oferecer uma fiabilidade e um conjunto de possibilidades mais amplo.

Um sistema de *mirroring*, ao contrário do que sucede com os discos rígidos, não tem necessariamente de se encontrar instalado nem na mesma máquina nem no mesmo local. Utilizando tecnologias de transmissão de dados de elevado débito, é possível criar uma solução de *mirroring* com repositórios de informação em, por exemplo, andares diferentes do mesmo edifício, ou em edifícios diferentes. São óbvias as vantagens desta possibilidade em termos de protecção contra desastres, uma vez que deixa de ser necessária a gestão, complexa, de *tapes* de *backup* armazenadas em locais remotos (*off-site*), bastando apenas transferir as operações para o suporte secundário. Para que esta solução possa ser considerada, é necessário que o suporte secundário se encontre a uma distância segura do primário. Contudo, à medida que as distâncias aumentam, também cresce o risco de criação de pequenos atrasos na escrita do suporte de apoio, originada pelos tempos de transmissão, ou seja, podem surgir situações em que os dados do suporte secundário não são precisamente iguais aos do primário. Para além disso, a escrita simultânea em dois suportes gera alguma latência nos tempos de processamento, uma vez que o controlador tem de esperar pela conclusão de dois processos de escrita.

Esta latência pode ser eliminada, aumentando para tal a complexidade da estrutura a utilizar. Se no caso apresentado (dois suportes), o processo de escrita das cópias de segurança é síncrono, na medida em que os dados são escritos em simultâneo em dois suportes, a introdução de um terceiro suporte e de um esquema de escrita assíncrona permitirá ter, por um lado, um desempenho adequado dos sistemas e, por outro, a replicação dos dados para localizações remotas, sem que tal interfira na produção.

Este *mirroring* assíncrono consegue-se, como referido, através da introdução de um terceiro suporte dos dados. Nesta configuração, os suportes primário e secundário são instalados relativamente perto um do outro (mas não necessariamente no mesmo local), a uma distância que não provoque latência nos tempos de escrita. A replicação entre estes dois suportes é síncrona, encontrando-se ambos permanentemente actualizados. De seguida, cria-se um processo de *mirroring* assíncrono, ou diferido, entre o segundo e o terceiro suporte, podendo a velocidade de transmissão de dados ser menos elevada. Esta é uma possibilidade complexa e potencialmente muito dispendiosa, apenas justificável quando os requisitos de disponibilidade da Empresa são extremamente elevados.

Na escolha da solução que melhor se adapte às suas necessidades, o responsável pela segurança deve equacionar todos os elementos disponíveis, incluindo o tipo de gestão possível (centralizada ou não), o grau de automatização desejado, os níveis de disponibilidade necessários, os ambientes a proteger, etc. Ao nível da selecção de uma tecnologia de salvaguarda de dados, deverão ser colocadas, entre outras, as seguintes questões:

- Que tipos de ambiente podem ser protegidos?
- Que tipo de gestão é oferecida:
  - individualizada (dos sistemas)?
  - centralizada a partir de uma consola de Administração?
- Qual o grau de facilidade de identificação dos suportes utilizados?

- Qual o grau de facilidade na recuperação dos dados?

Mais do que estas considerações técnicas, deverá igualmente ser implementada uma política de gestão de dados (já abordada), com vista à selecção da informação realmente importante, evitando por um lado o desperdício de recursos de armazenamento e salvaguarda e, por outro, o tratamento indiferenciado dos dados existentes.

Detecção de Intrusões

Uma fonte valiosa de informação sobre o que se passa na infra-estrutura informática da Empresa são os chamados "sistemas de detecção de intrusões", ou *Intrusion Detection Systems* (IDS). Estes sistemas nasceram com os computadores: no início, podiam não passar de um administrador a acompanhar a actividade da sua rede, tentando descobrir indícios de comportamentos fora do normal. Com o crescimento explosivo das capacidades e possibilidades associadas às tecnologias de informação, este tipo de detecção rapidamente se tornou impraticável e houve que desenvolver novas formas de acompanhar a actividade informática.

No início dos anos 90 do século passado começaram a surgir, como resposta a esta necessidade, sistemas automáticos que, em tempo real, analisam o tráfego e detectam (ou procuram detectar) tentativas não autorizadas de acesso à infra-estrutura lógica.

O grande objectivo destes sistemas é o de proporcionar uma visão sobre o que acontece na rede. Uma organização que possua *firewalls* e *routers*, devidamente configurados, poderá evitar a grande maioria dos ataques informáticos contra os seus sistemas. Porém, não possui qualquer tipo de conhecimento sobre o que acontece do lado de fora do seu perímetro, e desconhece o número de tentativas de intrusão oriundas do exterior. Por outro lado, um IDS não oferece apenas visibilidade ao que sucede no exterior do perímetro lógico da Empresa, mas revela igualmente o que acontece no seu interior: tentativas de acesso a servidores protegidos por parte de funcioná-

rios, etc. Para além desta capacidade, os IDS poderão reconhecer bem como evitar ataques informáticos.

Os IDS actualmente disponíveis podem ser divididos em dois grandes grupos: baseados em sistemas (HIDS – *host-based intrusion detection systems*) e baseados na rede (NIDS – *network-based intrusion detection systems*). Os primeiros são programas dedicados a sistemas individuais, afinados às suas características, e que detectam sinais de intrusão nas comunicações (de entrada ou de saída) dos sistemas que protegem. No caso de se tratar de um servidor de base de dados, por exemplo, o IDS poderá analisar, para além das transacções do sistema operativo e do protocolo de comunicações, operações específicas do motor de base de dados em utilização.

Relativamente aos IDS baseados na rede, estes assentam em "sondas", colocadas em pontos estratégicos da infra-estrutura, onde analisam todo o tráfego, comparando-o com uma base de dados de assinaturas de ataques para conseguir identificar actividades suspeitas.

Muitos dos sistemas existentes no mercado combinam estas duas fontes de informação, conseguindo deste modo uma visão muito mais abrangente da actividade dos SI. O único problema com a grande maioria da oferta é o facto desta se basear, um pouco como os sistemas antivírus, em bases de dados de assinaturas de ataques: se os ataques já conhecidos são detectados, as tentativas originais podem passar impunemente. Esta questão está a tentar ser solucionada através do desenvolvimento de sistemas "inteligentes" com a capacidade de cruzamento de dados e de aprendizagem baseada no historial de actividade detectada. Porém, ainda não existem soluções comerciais com estas características e pode-se presumir que a sua implementação ainda venha a demorar.

Outra questão potencialmente problemática tem a ver com o volume de dados gerado. Numa rede com elevados índices de actividade, os dados registados pelas sondas IDS podem atingir proporções significativas, o que implica dificuldades de capacidade de detecção

e de gestão. De facto, estes sistemas requerem acompanhamento em tempo útil por parte do respectivo administrador, como forma de validação das ocorrências registadas. Se considerarmos ainda que, para além destes, existem registos dos servidores, dos *routers*, das *firewalls*, dos sistemas antivírus, etc., a carga administrativa associada à sua gestão pode ser gigantesca. Nos casos em que se pretenda fazer uma gestão adequada da informação gerada pelos mecanismos de defesa da organização, todos estes dados deverão ser cruzados, com vista à detecção de padrões e à recolha de informações sobre (potenciais) ataques.

A instalação de um IDS deve ser meticulosamente ponderada. Regra geral, não são sistemas baratos e o seu preço sobe proporcionalmente às capacidades desejadas. Por outro lado, todo o tempo dedicado a um cuidadoso planeamento de instalação de um IDS irá, de futuro, poupar tempo precioso na gestão da informação gerada. Assim, os sensores de rede deverão ser instalados, em máquinas dedicadas, nos pontos de entrada da infra-estrutura de comunicação de dados e os sensores de sistema, logicamente, nos sistemas que se pretendem proteger. Todos estes sensores comunicam com uma estação de Administração central, onde são armazenados todos os dados registados. Esta estação, que também deverá ser dedicada a esta tarefa, é o ponto a partir do qual se faz a gestão centralizada dos recursos IDS disponíveis. Idealmente, toda a infra-estrutura IDS deverá pertencer a uma rede privativa, separada da rede de produção da Empresa, não devendo os computadores com sondas (de rede, naturalmente) ser visíveis nesta última, ou seja, as suas placas de rede não devem possuir qualquer endereço.

Por outro lado, as regras devem ser afinadas de modo a responderem às reais necessidades da organização.

Exemplo: nos casos em que não sejam disponibilizados serviços FTP, a detecção de ataques contra este protocolo poderá não se justificar.

Deste modo, para além de um sistema mais vocacionado para a realidade da infra-estrutura a proteger, consegue-se evitar a produ-

ção maciça de informação que, para além do ponto de vista académico, não possui interesse real.

Ao lidar com estes dados, é necessário confirmar a sua aplicabilidade, ou seja, verificar se não se tratam de falsos positivos: um falso positivo é a identificação de uma actividade legítima como sendo um ataque. O responsável pelo IDS deverá analisar os dados recolhidos e confirmar se se tratam, ou não de ataques reais. Os dados relativos à actividade maliciosa, registados pelo IDS, podem ocasionar várias reacções: alertas administrativos (incluindo chamadas para *beepers*) e reacções automáticas (como, por exemplo, interrupção da sessão ofensiva ou interdição do IP de origem).

Estas possibilidades fazem parte de um conjunto mais amplo de reacções, que serão abordadas de seguida.

Resposta a Ataques

Este tópico, não sendo exclusivo da segurança lógica, assume particular relevo neste campo, na medida em que é precisamente nesta área que o responsável pela segurança da Empresa terá de tomar algumas decisões complexas.

No caso da segurança física, a resposta a ataques encontra-se perfeitamente definida: no caso de um assalto, todos conhecemos bem os procedimentos a seguir, em resposta a esse acontecimento. Existem estruturas sociais, em funcionamento há muitos anos, apoiadas em legislação que evolui com alguma regularidade, que estão especificamente vocacionadas para dar resposta a questões relacionadas com ataques (independentemente da sua natureza ou escala) no mundo físico. No mundo lógico, esta é uma área ainda cinzenta.

São três horas da madrugada de um qualquer Sábado. O sistema de detecção de intrusões nos sistemas informáticos da Empresa acciona o *pager* do responsável pela segurança. Olhando para o código enviado pelo sistema, rapidamente se constata que a *firewall* foi comprometida e que, nesse preciso momento, alguém está a

gozar de livre acesso a servidores empresariais. Que fazer? Como actuar?

Não basta criar as infra-estruturas (técnicas ou humanas) de defesa da informação: é preciso definir procedimentos claros para reagir a acontecimentos como o descrito.

O guarda na recepção do edifício sabe (ou espera-se que saiba) o que fazer se alguém tentar entrar sem autorização, ou se algum sensor de movimentos detectar uma presença nas instalações quando não é suposto estar lá ninguém. Mas os administradores de rede sabem o que fazer se detectarem actividade não autorizada? Desligam os servidores? Tentam terminar a ligação do atacante? E se isso acontecer a meio da noite? E depois de resolvido o problema? Esquecem-no? Investigam-no? Comunicam-no às autoridades? A que autoridades?

Todas estas questões devem ser previstas e respondidas mesmo antes da ocorrência dos incidentes. As características actuais das redes de dados tornam estas decisões necessárias como resposta não à questão “se acontecer”, mas “quando acontecer”.

Qualquer organização que possua sistemas informáticos ligados em rede está exposta a ataques, quer sejam oriundos de *script kiddies* (pessoas sem grandes conhecimentos técnicos, que se limitam a descarregar software de ataque da Internet e a utilizá-lo aleatoriamente contra alvos indiscriminados), quer sejam da autoria de inimigos determinados, equipados e organizados, decididos a provocar estragos avultados ou a roubar informação confidencial. O número de tentativas de infecção ou de tentativas de descoberta de vulnerabilidades de um sistema ligado à Internet ascende diariamente às várias centenas, ou mesmo milhares, dependendo do perfil do sistema em causa. Uma organização com bastante projecção na sociedade atrairá naturalmente mais atenções do que uma pequena Empresa praticamente desconhecida. Mas ninguém está isento desta realidade. Como tal, torna-se necessário prever o maior número possível de ocorrências, bem como a respectiva resposta.

Esta reacção irá claramente variar, dependendo dos recursos ao dispor da organização. No caso de uma empresa com um núcleo de segurança informática, poderá existir uma clara definição de acções e de responsabilidades que entrarão em vigor sempre que se detecte um ataque. No caso de uma organização com poucos recursos humanos, dever-se-á igualmente definir, numa outra escala, o que fazer nestes casos.

Existem várias possibilidades, desde a criação de redes informáticas fictícias (*honey pots*), com o fim de atrair eventuais atacantes e de, aí, recolher o máximo de provas incriminatórias até à simples utilização de programas que interrompem a ligação ofensiva e a inserem numa "lista negra" de endereços aos quais é negado acesso. Mas um aspecto de suma importância, quer se trate de uma organização grande ou pequena, é a manutenção de rastos de auditoria adequados.

Esta questão já foi abordada, no início deste capítulo, relativamente à segurança física. No caso da segurança lógica, nunca é suficiente realçar a importância da manutenção de registos de auditoria.

Hoje em dia, praticamente todos os sistemas informáticos fornecem uma qualquer forma de registar a utilização que deles é feita. Estes registos, ou *logs*, constituem os elementos que permitem reconstituir acontecimentos e ter uma visão da utilização que é dada a determinado sistema. Assiste-se, em muitos casos, à definição pouco cuidadosa do que fica registado, do respectivo grau de pormenor e do que fazer a esses registos. De facto, muitos são os sistemas em que a definição de *logging* é rotativa, ou seja, ao fim de algum tempo, os registos mais recentes são sobrepostos a outros, mais antigos.

Deverá, pelo contrário, existir uma política de retenção de *logs* que defina não só a duração, volume e nível de detalhe desses registos, mas que estabeleça igualmente a sua remoção dos sistemas para locais seguros, ou para outros sistemas. Afinal, a última coisa que um atacante tipicamente faz, antes de deixar um sistema que acabou de penetrar, é eliminar o registo das suas actividades. Se este

for copiado, em tempo real, para outro sistema informático da Empresa, a sua eliminação num sistema não impedirá ao responsável pela segurança a reconstituição dos eventos.

Com uma regularidade definida, esses registos deverão ser retirados dos sistemas e, por exemplo, copiados para um suporte digital, guardado em local seguro. Esta manutenção histórica poderá permitir, por exemplo, determinar o início das tarefas de exploração que conduziram a uma tentativa de intrusão. Ou poderão revelar a partir de quando é que um elemento da Empresa começou a imprimir documentação confidencial. Esta tarefa, que consome pouco tempo e recursos, poderá ser um meio valiosíssimo de determinação de acontecimentos e um precioso auxiliar na obtenção de provas incriminatórias contra um delinquente.

Porém, deve ser dada particular atenção à definição do que deve ser registado. Se, em certos sistemas, é conveniente registar toda e qualquer actividade, outros, por exemplo, apenas necessitarão do registo de entradas e saídas no sistema e de acesso aos ficheiros do sistema operativo. Esta definição, se não for cuidadosamente realizada, poderá criar uma quantidade de dados que, simplesmente devido ao seu elevado volume, se tornam impraticáveis de gerir.

Os registos são, efectivamente, a última arma na linha de defesa (e de reacção) a ataques. São essenciais para determinar o que aconteceu, quando e como e são um instrumento fundamental na prossecução de acções punitivas.

Estas podem, e devem, ser equacionadas sempre que a organização considere haver lugar a retribuição pelos danos causados por um atacante, quer este seja um miúdo com tempo a mais nas mãos, quer se trate de um concorrente comercial.

A Secção Central de Investigação da Criminalidade Informática e Telecomunicações, na dependência da Direcção Central de Investigação da Corrupção e Criminalidade Económica e Financeira, da Polícia Judiciária, encontra-se especificamente dedicada à investigação de crimes electrónicos. Se bem que a legislação nacional

actualmente em vigor não seja abrangente, é possível, em termos legais, agir em resposta a ataques, sendo estes qualificados como "infracções económico-financeiras cometidas de forma organizada ou com recurso à informática".

O processo investigativo poderá envolver, entre outros, uma análise forense dos sistemas afectados, pelo que é de extrema importância a já referida retenção de *logs*, bem como a preservação cuidadosa dos sistemas, na medida em que estes poderão conter indícios reveladores da actuação do atacante, da extensão dos danos causados, etc. Uma breve pesquisa por "informática" no sítio da Polícia Judiciária na Internet revelará dezenas de comunicados de investigações, concluídas, sobre crimes informáticos, incluindo vários casos de detenção de indivíduos acusados de penetração ou utilização indevida de sistemas de terceiros.

No decurso da investigação, criminal ou oficiosa, de um ataque, será bastante natural que a Empresa se depare com intermediários, vítimas inocentes do atacante, utilizadas como "trampolins" para aceder aos alvos, servindo igualmente para dificultar a tarefa de determinação da origem do atacante.

Alternativamente, também se poderá deparar com "atacantes ingénuos", ou seja, terceiros que desconhecem o facto dos seus sistemas estarem a atacar outros.

As principais categorias de origens de ataques são, então, as seguintes:

- "*Zombies*": sistemas informáticos infectados com programas específicos, de controlo remoto, que são utilizados por terceiros para realizar ataques coordenados contra um alvo; o exemplo mais conhecido são os DDoS, ou ataques distribuídos de negação de serviços, em que grandes números de sistemas atacam simultaneamente um alvo com o objectivo de estrangular a sua ligação à Internet;

- Vermes (*worms*): sistemas infectados com programas específicos que tentam infectar automaticamente outros sistemas aos quais tenham acesso;
- Intermediários: sistemas comprometidos pelo atacante que, a partir deles, monta acções contra outras vítimas, com o fim de dificultar a sua detecção.

Claro que existem muitas outras possibilidades, incluindo atacantes ingénuos que tentam comprometer sistemas directamente a partir das suas máquinas pessoais, em casa, o que equivale a deixar uma assinatura e um cartão de visita nos sistemas atacados.

No meio de todas estas possibilidades, há que conseguir distinguir, na fase de rescaldo de um ataque, os "peões" e os "vilões". Normalmente, esta tarefa não é simples e, sem o sabermos, mesmo os nossos sistemas poderão ser utilizados num ataque contra terceiros. Esta realidade faz questionar algumas opções que actualmente se começam a colocar em termos de resposta a ataques. Existem já no mercado soluções que respondem automaticamente a tentativas de ataque, baseando-se no endereço IP de origem do atacante. Ora, como vimos, o atacante pode não passar de mais um elo numa cadeia de vítimas provocadas pelo verdadeiro malfeitor: ao responder indiscriminadamente contra o endereço IP registado como origem do ataque, podemos estar, sem o saber, a provocar outra vítima.

De facto, com a generalização deste tipo de sistemas, será fácil imaginar um novo tipo de ataque, extremamente eficiente e com riscos muito reduzidos para o seu autor. Por exemplo, se alguém quiser comprometer ou danificar os sistemas da Empresa XYZ, bastaria encenar algumas tentativas de ataque em nome dessa Empresa, contra terceiros. Estes, utilizando software de resposta automática, retaliariam contra a Empresa XYZ que seria, assim, alvo de vários contra-ataques sem sequer entender porquê.

É por este motivo que a capacidade de análise, o senso comum e o arbítrio humanos são indispensáveis na investigação. Todas as organizações e indivíduos que possuam sistemas ligados entre si,

nomeadamente na Internet, deverão, então, estar vinculados pelo princípio da inter-ajuda, fornecendo informação a terceiros sobre ataques originados nas suas máquinas. Este tipo de vínculo permitirá, logo à partida, alcançar dois resultados: se contactarmos alguém relativamente a um ataque oriundo de um sistema sob a sua alçada, estaremos a alertá-lo para o facto de ter uma ou mais máquinas potencialmente comprometidas, e poderemos, com base nos dados que nos forem fornecidos, prosseguir com a nossa investigação.

Claro que as coisas nem sempre são tão simples: há quem não queira colaborar, há quem não saiba como ajudar, enfim, existe uma série de variáveis que podem surgir, complicando todo o processo, particularmente se este envolver, como muitas vezes é o caso, sistemas alojados noutros países.

Para lidar com estas situações é, portanto, essencial estabelecer normas e procedimentos claros e específicos que tracem as linhas condutoras da Empresa. Não sendo possível prever todo o tipo de ataques que possam ocorrer, nem todas as formas de que estes se podem revestir, é fundamental que a organização saiba o que fazer. Poderá ser suficiente enviar uma mensagem de correio-electrónico ao administrador do sistema atacante, alertando-o para esse facto, ou a reacção pode chegar ao ponto de uma comunicação à polícia.

A decisão deve ser tomada caso a caso, auxiliada por um procedimento, e fundamentada na realidade da ocorrência, sempre bem enquadrada nas linhas mestras da segurança empresarial, ou seja, no Plano de Segurança da Empresa.

Segurança no Desenvolvimento

Este último tópico, a abordar no campo da segurança lógica, reveste-se de particular importância para todas as organizações que necessitem de desenvolver programas específicos para dar resposta às suas necessidades particulares.

O desenvolvimento de software poderá, dependendo das capacidades da Empresa, ser realizado por elementos do quadro da própria organização, ou poderá ser contratado a terceiros. Ambas as possibilidades possuem particularidades distintas, mas igualmente bastantes pontos em comum.

Quando se fala em segurança no desenvolvimento de software, não nos referimos apenas à inclusão de aspectos de segurança na fase de criação dos programas resultantes (como, por exemplo, controlo de acessos, diferenciação de utilizadores, etc.), mas também, e principalmente, aos aspectos relacionados com a verificação da segurança do código.

O ciclo de vida típico do desenvolvimento de software consiste tipicamente das seguintes fases:

- especificação;
- desenvolvimento;
- testes;
- correcção;
- testes de aceitação;
- entrada em produção.

O desenvolvimento de programas personalizados inicia-se com a fase de especificações, em que é definida a funcionalidade que se pretende que o software venha a ter, o modo como será utilizado, os resultados que deve produzir, etc. Nesta fase, é essencial incorporar todos os controlos de segurança que se deseja que o programa venha a ter. Como tal, a equipa de desenvolvimento, na fase de especificações, deverá interagir com membros da equipa de segurança, com vista à incorporação fluida dos controlos de segurança desejados. De notar que é sempre mais fácil, e mais vantajoso do ponto de vista funcional e monetário, incorporar estas funcionalidades na fase de definição, em vez de, posteriormente, ter de adaptar o código final.

Uma vez definidos os parâmetros que deverão reger o programa, inicia-se a fase de desenvolvimento. Nesta fase, e dependendo da complexidade do software (que poderá ir de uma base de dados relativamente simples, a um complexo sistema de, por exemplo, gestão de comércio electrónico), deverão ser realizadas auditorias ao código gerado. Estas análises terão como objectivo garantir a inocuidade do programa, tanto do ponto de vista da funcionalidade (o programa faz o que se pretende) como do ponto de vista da segurança (o programa não faz algo indesejado).

Finalmente, atinge-se um ponto do desenvolvimento em que surge uma versão funcional do programa. Nesta fase, procede-se ao teste inicial da aplicação, com a utilização de dados fictícios e com a simulação das várias possibilidades de funcionamento. Este é o momento decisivo para garantir a segurança do software desenvolvido. Ao procurar as falhas (*bugs*) existentes, muitas vezes apenas se tentam detectar aquelas directamente relacionadas com o funcionamento do programa. Acontece, porém, que os *bugs* relacionados com a segurança diferem dos *bugs* de funcionalidade, na medida em que estes últimos se prendem com algo que o programa não faz, ou faz mal, mas deveria fazer, enquanto que os *bugs* de segurança se manifestam tipicamente em acções adicionais, não pretendidas na especificação original. É nestes comportamentos adicionais que residem os principais riscos de segurança associados ao desenvolvimento, pois podem gerar falhas graves, no modo como, por exemplo, interagem com o sistema operativo.

Para a detecção destes erros, a equipa de desenvolvimento deverá olhar para além das especificações do software e tentar “olhar em volta”. Para este fim, deverão utilizar mecanismos de verificação do funcionamento do programa em desenvolvimento, mecanismos estes que devem permitir a indução voluntária de erros, a análise de interacções com outros programas, etc., como forma de obter uma imagem real do comportamento do programa.

Uma vez detectados os erros existentes na versão de teste, procede-se à sua correcção o que, por vezes, pode implicar a reescrita

de partes do código. No final desta fase de correcção, procedem-se a novos testes que, caso sejam bem sucedidos, servirão como mecanismos de aceitação do produto final.

Por fim, a aplicação é colocada em funcionamento no ambiente de produção da Empresa.

Todo o processo acima descrito é, como se constatou, complexo e implica a interacção de vários elementos, internos ou externos à organização. Para além disso, obriga igualmente à criação de um ambiente específico de desenvolvimento, que não deverá, nunca, ter contacto com o ambiente de produção existente, ou seja, toda a infra-estrutura de apoio ao desenvolvimento de software deverá encontrar-se separada da infra-estrutura de apoio às operações da Empresa, sob pena de interferências que podem ser danosas. Para além desta particularidade, e como vimos, deve-se prestar particular atenção a todas as fases do desenvolvimento, procurando não só garantir que o produto satisfaz os requisitos que levaram à sua criação, mas também que os aspectos relacionados com a segurança (embebida no próprio software ou relacionada com o seu comportamento) estão de acordo com as especificações da organização.

Dependendo da complexidade do software em desenvolvimento, e também do facto deste ser desenvolvido pela própria Empresa ou por terceiros, poderá inclusivamente surgir a necessidade da nomeação de alguém, não relacionado com o processo de desenvolvimento, que faça a auditoria do código. Este elemento poderá pertencer à organização ou, caso não exista essa capacidade, poderá ser um elemento externo, contratado especificamente para essa função.

Conformidade

Todos os aspectos relacionados com a Segurança Empresarial devem ser balizados por legislação ou normas aplicáveis.

Existe um corpo legislativo nacional que contém cláusulas condicionantes para a implementação das medidas de protecção referidas ao longo desta obra. Atendendo ao facto de alguma dessa legislação ser abordada no capítulo “Padrões e Legislação” deste livro, não nos iremos alongar a esse respeito nesta secção. Porém, é importante alertar para o facto de, para além da legislação, existirem diversas outras condicionantes que têm de ser tomadas em conta pelo responsável pela segurança, nomeadamente todos os requisitos de grupo ou de sector. Dependendo do ramo de actividade de cada organização, poderão existir normas específicas, aplicáveis a todas as empresas do mesmo ramo, que poderão ter de ser respeitadas. Tomemos como exemplo uma empresa do sector de prestação de cuidados de saúde.

Para além do dever de registar todas as bases de dados que contenham dados pessoais junto da Comissão Nacional de Protecção de Dados, a Empresa encontra-se obrigada a satisfazer uma série de requisitos, nomeadamente no que diz respeito ao acesso aos dados, e à protecção dos mesmos.

Este é apenas um breve exemplo de uma variedade de possibilidades que não podem ser esquecidas pelo responsável pela segurança da Empresa, sob pena de represálias legais que poderão ter efeitos devastadores sobre a organização.

Testes e Auditorias

Actualmente assiste-se a uma oferta crescente de serviços de teste e de auditoria de segurança, cujo objectivo é o de avaliar o grau de protecção dos sistemas informáticos das organizações. Quase toda esta oferta, senão mesmo toda, pode ser “personalizada” pelo

cliente, de modo a responder melhor às suas necessidades de análise.

Independentemente da importância destas análises e da pertinência dos seus resultados, o responsável pela segurança informática deverá escolher cuidadosamente a altura adequada para a sua realização, dependendo dos objectivos que pretenda atingir. Analisemos algumas possibilidades:

- Aquando da nomeação do responsável pela segurança: a Empresa contrata, ou nomeia, alguém para desempenhar as funções de responsável pela segurança. Uma das primeiras tarefas desse elemento poderá ser a de realizar uma análise de risco, ou contratar a terceiros uma auditoria de segurança, de modo a obter uma imagem, actual, do panorama de segurança da organização. Os resultados desta auditoria servirão de ponto de partida para a elaboração de soluções e para a correcção das insuficiências detectadas.
- Após a implementação de medidas de segurança: Partindo do princípio de que o responsável pela segurança tem um conhecimento mais ou menos aprofundado da situação da Empresa, em termos de segurança lógica, este poderá tomar medidas preventivas e/ou correctivas, no âmbito do Plano Global de Segurança. Neste caso, os testes ou auditorias de segurança têm como objectivo avaliar a eficácia das medidas introduzidas e validar as decisões tomadas.
- Com regularidade temporal: Em paralelo ao desenvolvimento e implementação do Plano Global de Segurança, o responsável por esta poderá optar por um acompanhamento das medidas implementadas através de testes ou auditorias regulares à segurança. Poderá, deste modo, ter uma imagem mais real das consequências dos mecanismos adoptados e adequar a introdução de novas soluções a estes resultados. Por outro lado, a obrigatoriedade deste tipo de auditorias regulares pode ser um requisito da própria organização.

Para além destas possibilidades, muitas outras existirão, tais como testes pontuais a aspectos específicos da segurança lógica, planos estruturados de auditorias parciais aos vários sistemas informáticos existentes e por aí adiante.

A decisão de realizar um teste ou uma auditoria aos sistemas, bem como a altura adequada para a sua execução, dependem das circunstâncias específicas da Empresa, bem como do orçamento disponível, pois estes serviços, quando contratados, não são propriamente baratos.

Existem várias possibilidades de testes e auditorias, das quais abordaremos algumas de seguida.

Auditoria Completa aos Sistemas

Sem dúvida a opção mais completa e abrangente, esta é, também, a mais dispendiosa. Consiste na análise exaustiva de todos os sistemas informáticos da Empresa, tanto externos (expostos na Internet), como internos.

Uma auditoria desta natureza poderá demorar, dependendo do tamanho da Empresa, bem como do número de sistemas a analisar, entre algumas semanas a vários meses. Convém, contudo, garantir que a auditoria não se prolongue por muito mais de um mês pois, atendendo ao ritmo da evolução tecnológica (e ao ritmo de divulgação de vulnerabilidades e medidas correctivas), alguns dos dados poderão perder a sua actualidade.

Este tipo de análise utiliza uma combinação de processos automatizados (por exemplo, detectores de vulnerabilidades) e de processos humanos. Convém garantir que a realização de testes não seja intrusiva, ou seja, é necessário ter a certeza de que nenhum teste irá prejudicar as máquinas de produção. Para além disso, o cliente deverá poder optar por uma análise “às claras” ou “às escuras” da sua infra-estrutura ligada à Internet. No primeiro tipo de avaliação, são reveladas as características (endereços IP, diagramas de rede, tipo de sistema operativos, aplicações, etc.) das máquinas a anali-

sar, enquanto que no segundo tipo apenas é fornecida a gama de endereços IP detida pela Empresa.

Os resultados desta auditoria poderão ser bastante volumosos. O responsável pela segurança deverá garantir que, por muito exaustivos que sejam, os relatórios resultantes sejam úteis. É discutível a utilidade de dezenas de páginas com o *output*, não processado, de um qualquer programa de varrimento de portas e serviços de servidores – o cliente deverá certificar-se de que todos os resultados sejam comentados por quem realiza a auditoria, bem como de que o relatório irá conter recomendações pragmáticas e claras para a correcção das deficiências encontradas e para o aperfeiçoamento das medidas existentes.

Testes de Intrusão

Os testes de intrusão não são mais do que tentativas de acesso aos sistemas da Empresa por parte de pessoas não autorizadas. Este tipo de análise poderá ser realizado sem qualquer conhecimento prévio dos sistemas a testar, ou com a indicação das respectivas características. Ambas as possibilidades têm pontos positivos e negativos: no caso da primeira, cria-se um cenário mais realista, na medida em que assumirá o ponto de vista de um hipotético atacante; no caso da segunda, em que existe o conhecimento completo das características dos sistemas a testar, garante-se a exaustividade dos testes, pois estes irão provavelmente deixar menos vulnerabilidades de fora.

Estes testes podem ser realizados tanto a partir do interior da rede da Empresa, como a partir da Internet, dependendo a decisão sobre o ponto inicial do teste, das características da organização (número de sistemas, número de funcionários, tipo de aplicações) e dos proveitos que possam ser obtidos da análise.

Em qualquer dos casos, convém, mais uma vez, garantir que os testes não sejam intrusivos e que os resultados sejam úteis, e não apenas descrições de ataques.

Detecção de Vulnerabilidades

Este é um teste de simples execução, constando do confronto dos sistemas e aplicações existentes com listas de vulnerabilidades conhecidas. Atendendo ao enorme número de vulnerabilidades existentes, estes testes são normalmente realizados com programas automáticos de detecção, contendo bases de dados de vulnerabilidades actuais.

Caso o responsável pela segurança da Empresa opte pela contratação de um serviço deste tipo, ou pela aquisição de um *scanner* de vulnerabilidades, deverá ter em conta as especificidades da sua organização, devendo certificar-se da utilidade do teste. Se apenas existem sistemas Unix na Empresa, um teste destes cujas características apontem fundamentalmente para sistemas operativos da Microsoft poderá não ser muito útil.

Um extra que um serviço, ou aplicação, destes deverá conter é a correcção automatizada e/ou manual (no caso de serviço contratado) das vulnerabilidades detectadas, bem como um registo pormenorizado das acções realizadas.

Detecção de Pontos de Acesso Telefónico

Muitas vezes apelidados de “testes de *war-dialing*”, este teste consiste fundamentalmente na realização de varrimentos a todas as linhas telefónicas da Empresa, com vista à detecção de modems ou servidores de acesso, autorizados ou não. Este teste deverá, ainda, incluir tentativas de intrusão nos sistemas ligados a esses pontos de acesso. Para além do varrimento telefónico, poderá ser realizado um varrimento aos sistemas informáticos existentes, com vista à detecção de eventuais pontos de entrada.

A pertinência de um teste deste género é particularmente elevada no caso de organizações muito grandes ou geograficamente dispersas, em que não seja possível exercer controlo sobre todas as estações de trabalho existentes. O comodismo de muitos utilizadores

poderá levar à instalação de *modems* ou à disponibilização de serviços que podem constituir pontos de entrada alternativos na rede empresarial.

Detecção de Pontos de Acesso WLAN

Muitas vezes apelidado de "*war-driving*", este teste consiste na procura sistemática de pontos de acesso *wireless* piratas, eventualmente instalados por utilizadores, à revelia do departamento de informática (por exemplo, por alunos num campus universitário). Pode também representar a tentativa sistemática de detecção de pontos de entrada desprotegidos nas redes *wireless* empresariais. A tecnologia actualmente existente permite realizar estas acções de uma forma (relativamente) simples e discreta, o que obrigará as organizações a ter especial cuidado na configuração dos aspectos e funcionalidades de segurança destas redes.

Engenharia Social

Este teste tem como objectivo detectar o grau de vulnerabilidade da organização a "ataques sociais". Poderá ser realizado pelo responsável pela segurança, por outros elementos da Empresa ou por prestadores deste tipo de serviços: existem empresas no mercado que os oferecem, como pacotes isolados ou como parte de auditorias mais amplas.

Pode ser composto por um conjunto simples de tentativas de obtenção de informação através, por exemplo, do telefone, ou poderá incluir acções mais complexas como tentativas de entrada nas instalações.

Exemplo: - "Bom dia. Sou o engenheiro do <fornecedor de serviços de telecomunicações da Empresa-alvo> e estou a fazer testes na central da vossa zona. Preciso que me indique se existem modems ligados às vossas linhas e quais os respectivos números."

- Na entrada do edifício, caso exista guarda, um elemento da equipa de testes poderá entrar em velocidade acelerada, sem parar para se identificar. Caso o segurança se levante e o tente deter, entrará outro elemento que, por sua vez, tentará aceder ao interior das instalações, aproveitando o momento de desatenção do guarda, que está ocupado a tentar deter o primeiro intruso.

São testes simples e que poderão surtir efeitos surpreendentes.

Independentemente do tipo de teste ou auditoria que se decida fazer, e da altura em que este venha a ser realizado, o importante é conseguir enquadrar este investimento nos objectivos do Plano Global de Segurança da Empresa. Estas actividades devem ser realizadas com o objectivo de obter vantagens pragmáticas. Para tal, o responsável deverá calcular cuidadosamente a melhor altura para a realização destes exercícios, bem como o processamento e integração posterior dos respectivos resultados. Se existem testes, como a detecção de vulnerabilidades, que produzem efeitos quase imediatos (como a eliminação das vulnerabilidades detectadas), outros, como os testes de engenharia social, implicam esforços de sensibilização, prévios ou posteriores, junto da comunidade de colaboradores da Empresa.

Acima de tudo, e independentemente da realização dos testes por elementos internos ou externos à Empresa, trata-se de um investimento de tempo e dinheiro, por vezes significativo, que deverá gerar o maior retorno possível para o negócio.

Conclusão

Este capítulo abordou diversos aspectos da segurança, indicando as suas principais características ou, pelo menos, alguns dos conceitos que importarão reter aquando da criação do Programa de Segurança.

Como nota final, importa referir que os elementos da segurança lógica aqui introduzidos tiveram apenas como objectivo proporcionar uma visão panorâmica das possibilidades actualmente existentes. A evolução tecnológica, como já foi repetidamente referido, é um processo extremamente veloz que, se por um lado conduz à rápida maturação dos produtos, por outro pode levar à sua obsolescência. Deste modo, a introdução de novas tecnologias na Empresa reveste-se de características particulares, que serão abordadas mais adiante neste livro (ver “Implementação”, no capítulo “Gestão do Programa de Segurança”), não podendo o responsável pela segurança dos SI deixar de ponderar cuidadosamente todas as decisões nesta matéria.

Capítulo IV - Segurança Face ao Desastre

A área de segurança face ao desastre é actualmente um tema quente, sobre o qual incide regularmente a atenção dos meios de comunicação desde os trágicos atentados às torres gémeas nova-iorquinas, a 11 de Setembro de 2001, e com renovado vigor a cada desastre natural ou induzido pelo Homem.

A protecção face ao desastre requer antecipação, uma vez que, quando o desastre bate à porta, regra geral já é demasiado tarde para impedir que a situação, potencialmente calamitosa, degenere, encontrando-se o grau de controlo que detemos sobre o evento directamente relacionado com os meios funcionais, materiais, humanos e logísticos que foram garantidos antecipadamente.

A forma mais fácil de responder à questão “porquê investir na protecção contra desastre” vem de um estudo realizado nos Estados Unidos pela *Federal Emergency Management Agency* que refere que, consoante a natureza do desastre, 25% a 40% das empresas não volta à actividade após um acidente de grandes proporções.

Neste capítulo iremos abordar as diversas fases do desastre e discutir várias estratégias para a protecção dos sistemas de informação e restantes componentes do negócio.

Anatomia de um Desastre

Um desastre consiste num acontecimento imprevisto que origina perdas e dificuldades à organização, afectando significativamente, de forma negativa, a sua capacidade para executar serviços essenciais. A quantidade de possibilidade de concretização destes acontecimentos apenas encontra paralelo na variedade das formas como são produzidos danos.

Tipos de Desastre

Os desastres podem ter as mais diversas origens, embora estas se enquadrem tipicamente no seguinte conjunto:

- fenómenos ou outras causas naturais (ventos ciclónicos, terramotos, inundações, etc.);
- incêndios;
- explosões;
- falhas de energia;
- falhas mecânicas;
- falhas infra-estruturais;
- distúrbios sociais (tumultos, manifestações, guerras, etc.);
- erros humanos;
- crimes;
- acidentes biológicos ou químicos;
- impactos de veículos terrestres/aéreos/navais.

Uma vez que o impacto de um incidente varia consoante a vulnerabilidade da Empresa, o mesmo incidente poderá representar, para empresas diferentes, um desastre ou apenas uma inconveniência. Consoante os casos, a capacidade de recuperação, ou de alta disponibilidade, pode representar tanto uma garantia de sobrevivência como um factor de competitividade.

Cronologia

Nem todos os incidentes resultam num desastre: a maioria provoca apenas um pequeno período de indisponibilidade, ou seja, uma emergência. Um desastre resulta de um incidente que afecte a capacidade da organização em realizar as actividades de suporte aos seus processos críticos, durante um período superior ao limite

máximo tolerado pelas funções do negócio. Ou seja, enquanto as funções da Empresa suportarem a paragem ou indisponibilidade de alguns processos de suporte, o incidente é considerado uma emergência. Este passará a desastre a partir da "declaração de desastre", altura em que a organização assume inequivocamente a necessidade de activação de medidas excepcionais conducentes à recuperação dos processos e actividades afectados pelo incidente. Em caso de desastre, o principal objectivo do negócio será, então, o de retomar todas as suas actividades críticas o mais rapidamente possível, o que acontecerá no período de recuperação. Só no final deste período serão retomadas as restantes actividades, não críticas, entrando a Empresa, assim, na fase de regresso à normalidade. A Fig. IV-1 apresenta esquematicamente o desenrolar cronológico de um acidente, representando as várias fases: perda de funções críticas, declaração de desastre, recuperação das funções críticas e regresso à normalidade.

O objectivo da criação de um plano de recuperação ou continuidade do negócio é, então, o de garantir que a recuperação das funções críticas da Empresa ocorra de forma suficientemente rápida, de modo a garantir que a sua viabilidade não é comprometida.

A promoção da segurança em caso de desastre terá sempre lugar a montante do incidente que o origina, apesar de ser composta tanto por acções de prevenção, que visam diminuir a probabilidade de ocorrência dos incidentes que possam originar um desastre, como por medidas de protecção, reduzindo neste caso o impacto da ocorrência do desastre sobre a Empresa.

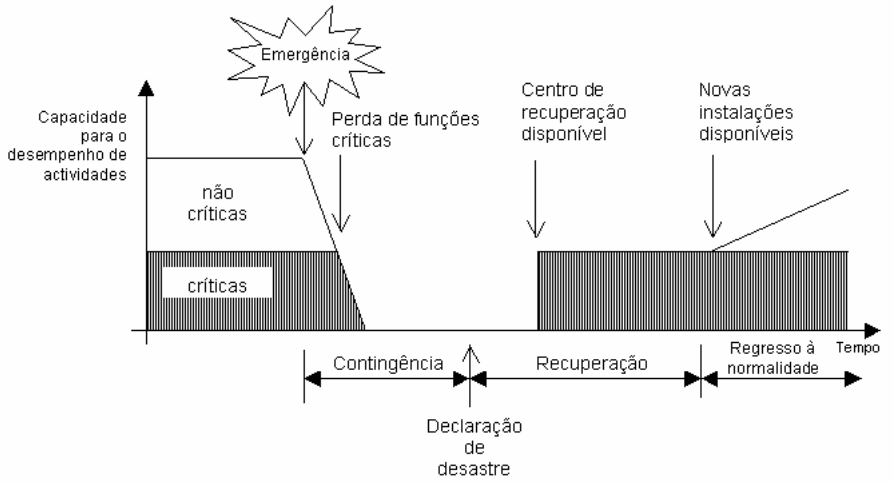


Fig. IV-1: Fases de um desastre

Planeamento da Recuperação ou Continuidade do Negócio

O projecto de planeamento da recuperação ou continuidade do negócio visa identificar as actividades a executar em caso de desastre, os responsáveis pela sua execução, os meios necessários e o modo de realização dessas actividades.

Este projecto é constituído por cinco fases:

1. arranque;
2. redução de riscos e avaliação do impacto;
3. desenvolvimento do plano;
4. implementação do plano;
5. manutenção e actualização.

O sucesso do projecto é condicionado por vários factores estratégicos, inteiramente dependentes da Empresa, que reflectem o modo como as instâncias decisórias da organização assumem, ou não, a

importância das medidas de prevenção e protecção. Por este motivo, o projecto deverá ter o empenhamento inequívoco da Administração, que o deve incorporar no plano estratégico do negócio.

Com base neste empenhamento inicial, os seguintes factores devem ser previstos e providenciados:

- os dados críticos da Empresa devem ser armazenados em instalações separadas (*off-site*);
- os meios de recuperação devem estar disponíveis no prazo necessário;
- o plano deve ser actualizado regularmente;
- o plano deve ser testado com regularidade;
- o plano deve ser abrangente.

Cada uma das fases atrás indicadas será apresentada de seguida, sendo identificados os seus principais aspectos.

Arranque do Projecto

A fase de arranque do projecto de recuperação ou de continuidade do negócio é caracterizada pelo respectivo enquadramento, pela definição dos seus objectivos e âmbito, bem como pela identificação dos pressupostos e terminologia base. Nesta fase também se define um modelo de gestão para todo o projecto.

Objectivos, Âmbito, Pressupostos e Terminologia

O principal objectivo de qualquer plano de recuperação de desastre ou de continuidade do negócio é, naturalmente, reagir a um desastre de modo a reduzir as suas consequências para um nível considerado aceitável pela Empresa. No entanto, este importante objectivo carece de definição, pois o que é entendido por “redução”, “consequências”, “desastre” e “aceitável” varia significativamente,

obrigando deste modo à definição exacta do que se pretende venha a ser o retorno do esforço associado à realização do projecto. Estas definições deverão ser transpostas para um documento que possa servir de referência a todos (potencialmente muitos) os elementos envolvidos: deste modo, toda a organização, desde a Administração aos técnicos, possuirá referências comuns.

É em sede de definição de objectivos, e mais precisamente na definição das "consequências" a mitigar, que se devem identificar os requisitos nas mais diversas matérias (temporais, de imagem comercial, legais, regulamentares, etc), a cumprir que permitem prevenir as consequências identificadas.

Exemplo: em caso de desastre, uma empresa de prestação de serviços de saúde tem como requisito salvaguardar todas as bases de dados com informação clínica dos seus clientes, mantendo o cumprimento das obrigações legais relativas à protecção de dados pessoais (Lei n.º 67/98, de 26 de Outubro). Para além disso, tem de conseguir comunicar aos seus parceiros e clientes (e ao público em geral) que é capaz de garantir a protecção e recuperação desses mesmos dados.

É igualmente necessário identificar o que se pretende obter em termos de redução, quer da probabilidade da ocorrência do desastre (prevenção), como do seu impacto (protecção).

Exemplo: deverão ser criados mecanismos de detecção e extinção de incêndios (prevenção), bem como criadas zonas com portas corta-fogo para armazenamento de informação crítica (protecção).

À definição dos objectivos do projecto importa acrescentar a definição do respectivo âmbito. Este último destina-se a limitar o alcance do projecto, impedindo que este se atole em detalhe excessivo, ou entre em pormenores que dificilmente se venham a verificar justificados ao nível do custo final. Esta definição também deverá incluir a

definição do que é "crítico", através do recurso a métricas quantitativas sempre que possível. Outro dos aspectos importantes na definição do âmbito prende-se com a selecção do tipo de protecção pretendida pela Administração da Empresa.

As expressões "plano de recuperação" e "plano de continuidade", se bem que possam, à primeira vista, parecer sinónimos, reflectem duas posturas distintas perante o desastre. A principal diferença entre estas duas formas de protecção (recuperação/continuidade) consiste no foco da análise de risco e impacto que é realizada no âmbito da protecção. Quando a visão empregue é tecnológica, o que iremos proteger são os sistemas, pelo que o impacto dos riscos é avaliado com base na premissa que um determinado sistema pode ficar indisponível. Quando a visão é funcional, o que iremos analisar é o impacto da indisponibilidade de uma actividade de suporte sobre uma função crítica, podendo essa actividade ser tecnológica ou não. Um factor que deve ser considerado é o facto da capacidade de sobrevivência de uma determinada actividade TI ao desastre não implicar necessariamente a garantia da sobrevivência de qualquer um dos processos que sobre ela assentam. Na realidade, considera-se frequentemente que os SI são a pedra basilar que sustenta a recuperação do desastre, sendo igualmente encarados, regra geral, como um primeiro nível de protecção. Naturalmente, a protecção acrescida oferecida pela continuidade do negócio tem um custo como contrapartida: o esforço extra associado ao planeamento da recuperação de um conjunto mais alargado de sectores da Empresa[11].

Para além da definição do âmbito do projecto, a identificação dos pressupostos sobre os quais este assenta representa uma forma

---

[11] Uma vez que o projecto de recuperação de desastre é um subconjunto (focado nos sistemas de informação) do projecto de continuidade do negócio, no resto deste capítulo será tratado explicitamente o planeamento da continuidade do negócio, por uma questão de simplicidade e abrangência.

adicional de conter o seu alcance: os pressupostos devem definir o cenário de desastre para o qual o plano será concebido, bem como especificar a amplitude geográfica do desastre e a dimensão ou impacto previstos sobre a Empresa e sobre a infra-estrutura que a suporta (linhas de comunicação de voz e dados, fontes de energia, acessos, pessoal, etc.).

Uma vez delineado o contorno do projecto resta proceder à definição inequívoca da terminologia a empregar, uma vez que o significado dos vários termos relacionados com matérias de protecção de desastre não é consensual. Um exemplo desta disparidade de significados possíveis é o termo "recuperação de desastre" que é empregue em meios diferentes com o significado de "recuperação de desastre TI", "continuidade do negócio" e "continuidade do negócio com alta disponibilidade". No final deste livro encontra-se uma lista de terminologia que pode ser utilizada como base para esta componente da fase do projecto de continuidade do negócio, informação essa que pode ser complementada por uma pesquisa nos glossários existentes na Internet.

Modelo de Gestão do Projecto

A gestão do projecto de continuidade do negócio deve ser efectuada segundo uma metodologia comprovada, com a qual os vários membros da equipa se sintam confortáveis, e que seja suportada por um documento que contenha:

- a descrição da situação actual da Empresa em matéria de protecção de desastre;
- os objectivos, âmbito, pressupostos e terminologia (abordados anteriormente);
- os benefícios que se pretendem obter com o projecto;
- o planeamento das actividades de alto nível;
- a descrição da equipa que o irá executar;

- os produtos finais;
- os riscos; e
- o orçamento do projecto.

Para cada actividade de alto nível apresentada deverão ser definidos os respectivos objectivos, metas, âmbito e riscos de desvio ao planeamento, tanto orçamentais como ao calendário.

Esta definição de pormenor pode ser traduzida numa lista em que deve ser inserido o maior número possível de elementos relacionados com a actividade em questão.

Exemplo: ACTIVIDADE: Levantamento de Funções Críticas

TAREFAS

1. Identificação das áreas de negócio da empresa.
2. Identificação dos interlocutores responsáveis por cada área.
3. Criação de um modelo quantitativo/qualitativo unificado, de classificação das funções.
4. Criação de questionários uniformes para recolha de informação.
5. Reuniões com os interlocutores identificados em 2, com aplicação do modelo de classificação e dos questionários.
6. Validação das respostas obtidas.
7. Cruzamento dos dados levantados durante as reuniões.
8. Prioritização das funções de negócio de acordo com o seu grau de criticidade.

Nota: este exemplo pretende apenas ilustrar o tipo de tarefas associadas a uma actividade de alto nível, não pretendendo ser exaustivo. Esta listagem deveria ainda incluir a indicação das pessoas responsáveis por cada tarefa e, se possível, o calendário previsto.

Este processo de gestão, que será abordado em maior profundidade em "Gestão do Programa de Segurança" sob outra óptica, deverá detalhar e estruturar o trabalho, identificando processos de aprovação pela Administração, de definição e gestão de equipas, metodologias de *reporting* (quem, o quê, a quem) e de atribuição de tarefas.

O modelo de gestão utilizado deverá ainda estabelecer o processo de identificação de desvios ao planeamento, quer pela verificação da conclusão das tarefas como pela realização de avaliações intercalares, devendo também prever a introdução dos ajustes necessários, tais como a alteração da sequência das tarefas ou a redução/ampliação do seu âmbito. O modelo empregue deverá ainda contemplar a avaliação das actividades executadas e permitir o aproveitamento dos ensinamentos recolhidos nas várias tarefas.

Redução de riscos e avaliação do impacto

A segurança face ao desastre é conseguida à custa de medidas que evitam tanto a ocorrência do desastre como danos significativos daí resultantes.

A primeira consiste num acto de prevenção que toma lugar antes de ocorrer o incidente que origina o desastre. A segunda ocorre tanto antes como depois do incidente, requerendo o posicionamento antecipado de mecanismos e procedimentos que permitam limitar o seu impacto. Estas medidas são tomadas quer durante a contingência, quer nas fases de recuperação e regresso à normalidade, nos

casos em que o incidente provoque mais do que uma mera indisponibilidade.

Análise de Risco

Atendendo a que o grau de risco efectivo é determinado pela probabilidade de concretização de um ataque e pela vulnerabilidade existente a esse ataque (ver "Análises de Risco e de Impacto" em "Gestão do Risco"), e considerando que a probabilidade de ocorrência dos ataques se encontra, regra geral, fora do controlo da Empresa, as medidas de prevenção destinadas a reduzir riscos irão actuar fundamentalmente junto das vulnerabilidades. Para tal, será necessário realizar uma análise de risco, empregando uma das metodologias anteriormente expostas.

A análise de risco realizada no âmbito do planeamento da continuidade do negócio visa, então:

- identificar as ameaças que podem estar na origem de desastres, ou seja, que podem afectar as principais actividades;
- determinar as vulnerabilidades existentes que aumentam a probabilidade de concretização dessas ameaças; e
- calcular a probabilidade de ocorrência das ameaças identificadas face às vulnerabilidades detectadas.

Após a obtenção destes elementos, os riscos podem ser ordenados, permitindo assim a definição de prioridades para as medidas de prevenção a implementar.

Nesta fase pretende-se que a análise seja realista, ou seja, que não tente abarcar todos os riscos possíveis. Caso o tente, para além de se transformar numa tarefa virtualmente interminável, perderá a sua validade, uma vez que os seus resultados apenas possuirão interesse de um ponto de vista meramente académico.

Controlo de Riscos

As medidas de prevenção contra os riscos são designadas "controlos", sendo necessário introduzi-los durante o planeamento da continuidade do negócio, como forma de reduzir antecipadamente o potencial de concretização de perdas. Para além disso, acarretam o benefício adicional de permitir a redução dos prémios pagos em seguros contra desastre[12].

A introdução de controlos deve ser efectuada com base na prioritização conseguida através da análise de risco já referida e deve privilegiar os princípios da segurança apresentados anteriormente em "Princípios de Prevenção e Protecção", no capítulo "Teoria da Segurança", dos quais decorre a necessidade de realizar uma análise de custo/benefício. Esta introdução pode ser realizada no âmbito mais alargado do Programa de Segurança da Empresa, ou enquadrada unicamente pelo projecto de continuidade do negócio, antes da fase de criação dos planos.

Exemplo: entre os controlos enquadrados pelo projecto de continuidade do negócio encontra-se a introdução de políticas, planos e procedimentos de redução de riscos, de sistemas de extinção de fogo, de fontes de alimentação ininterrupta e de procedimentos de controlo de acesso físico, entre outros.

Análise de Impacto no Negócio

Conforme referido anteriormente em "Análises de Risco e de Impacto" no capítulo "Gestão do Risco", a análise de impacto no

---

[12] No século XIX, a introdução maciça de "*sprinklers*" em fábricas de têxteis deveu-se precisamente ao facto das empresas seguradoras terem concluído que as fábricas assim protegidas corriam menos riscos e, como tal, deveriam ser beneficiadas em termos de prémios de seguros.

negócio visa apurar quais as actividades (tecnológicas ou não) críticas para o funcionamento da Empresa.

O cumprimento dos Tempos Alvo de Recuperação (TAR) das funções críticas para o negócio requer a utilização de estratégias distintas para cada grupo de TAR definido. No exemplo utilizado, estas estratégias seriam, por exemplo, alta disponibilidade para o primeiro grupo, a utilização de um *hot-site* para o segundo e de um *cold-site* para o terceiro[13]. As diversas estratégias de recuperação serão abordadas de seguida.

Desenvolvimento do Plano

O plano de continuidade do negócio é um documento único, composto por um conjunto de outros documentos, dependendo a sua composição exacta dos objectivos e âmbito definidos, bem como da estrutura precisa da Empresa e da distribuição das funções críticas no seu seio.

Uma característica importante do plano (ou procedimento) deverá ser a sua flexibilidade e independência, uma vez que um plano difícil de alterar, ou seja, com uma lógica particular e pressupostos muito específicos, poderá dificultar mais do que ajudar numa situação de desastre. Neste caso, ao esforço de tentar fazer funcionar o plano inflexível desadequado, acresce a necessidade de criação (durante o desastre) de um plano alternativo. Adicionalmente, um plano com pontos únicos de falha (por exemplo, dependente de uma única pessoa) será mais facilmente inviabilizado em circunstâncias reais.

---

[13] O conceito *hot* e *cold-site* será desenvolvido mais adiante neste mesmo capítulo.

O plano de continuidade do negócio deve englobar planos de:

- contingência, recuperação e regresso à normalidade contendo:
  - procedimentos para cada processo e actividade críticos;
  - estrutura e constituição das equipas que os irão executar;
  - plano de acção (diagrama de execução);
  - informações auxiliares (por exemplo, contratos, listas de contactos, etc.);
- gestão de crise, descrevendo o funcionamento do:
  - centro de operações (quem coordena);
  - centro de comando (quem decide);
- testes;
- exercícios;
- actualização do plano;

Antes de se iniciar o desenvolvimento dos diversos planos é necessário proceder à identificação de estratégias alternativas que permitam cumprir os requisitos de recuperação das funções, processos e actividades críticos, apurados na análise de impacto no negócio. Uma vez delineadas, essas estratégias deverão ser analisadas, servido esta análise de base para o processo de selecção levado a cabo pela Administração. Depois de aprovadas, estas estratégias deverão ser consolidadas numa estratégia global sobre a qual irão assentar todos os planos necessários à protecção da Empresa.

Estratégias de Protecção

A criação de uma estratégia de protecção inicia-se com o levantamento dos requisitos materiais, funcionais, infra-estruturais e de

dados necessários ao funcionamento das actividades críticas, tecnológicas ou não.

O passo seguinte será a identificação de alternativas estratégicas para a recuperação de cada função e processo. As principais alternativas existentes ao nível da protecção contra desastre estão relacionadas com as diversas opções disponíveis relacionadas com:

- a degradação do funcionamento aceite (tecnologia e meios afectos à protecção);
- a entidade responsável pelos serviços de recuperação (interna, comercial, acordos entre empresas ou estratégia mista);
- o tipo de instalações de recuperação (*hot/warm/cold site*).

As escolhas realizadas nestes domínios irão ditar não só os custos associados à implementação e manutenção do plano, mas também os tempos de resposta em caso de desastre (ver Fig. IV-2).

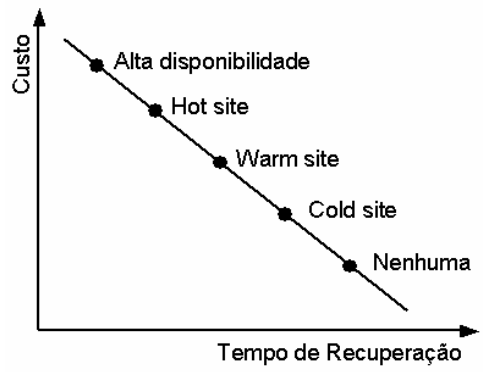


Fig. IV-2: Estratégias de recuperação: TAR vs. Custo

Depois de identificadas e definidas, as estratégias deverão ser avaliadas, considerando:

- se permitem cumprir os TAR apurados na análise de impacto no negócio;
- os custos e benefícios associados à estratégia;
- as vantagens estratégicas ou competitivas que possam sobrevir;
- a capacidade de sobrevivência conferida; e
- a preservação de valores intangíveis (tais como imagem da marca, lealdade ou preferência dos clientes, etc.).

Esta avaliação deverá ser consolidada numa lista com as vantagens e desvantagens das diversas alternativas, que servirá de base à justificação das propostas apresentadas à Administração para cada área (protecção de dados, de sistemas, etc.).

De entre os activos da Empresa, os seus dados serão, na vasta maioria dos casos, um dos bens mais preciosos. Sem a preservação dos dados vitais, ou seja, do conjunto de dados necessários às actividades de suporte críticas, dificilmente o negócio da Empresa poderá prosseguir e esta incorrerá, na melhor das hipóteses, em custos significativos para a recriação dessa informação. As estratégias de recuperação de dados, assentes nas tecnologias de cópia de segurança indicadas anteriormente em “Segurança Lógica”, no capítulo “Áreas da Segurança Empresarial”, deverão ser definidas de modo a garantir não só a recuperação dos dados, mas também da informação e, sempre que possível, do conhecimento deles extraído.

Exemplo: imagine o seguinte caso simplista. Após um desastre dirige-se ao centro de recuperação que contratou antecipadamente, recupera os dados que copiara na véspera e que expedira para fora da Empresa, obtendo, assim, um ficheiro com milhões de números, separados por vírgulas. Estes números representam algo, mas não sabe bem o quê. Os dados estão lá. O que falta é a informação que os permitirá usar: a formatação e significado dos campos.

Ao definir a estratégia de protecção dos dados dever-se-á ter particular cuidado em garantir a integridade e confidencialidade das cópias, protegendo-as, durante o transporte e armazenamento, contra perigos físicos (como o fogo, furto, desmagnetização ou inundação). Para garantir a sua utilidade será essencial armazenar as cópias longe do local em que se encontram os sistemas de informação de onde os dados foram retirados. Esta precaução reveste-se de particular importância uma vez que, caso contrário, mesmo que as cópias permaneçam intactas após o desastre, o acesso aos suportes da cópia poderá ser impossível durante vários dias, bastando para tal que a estrutura do edifício, ou os meios de acesso, sejam comprometidos pelo desastre.

A recuperação de sistemas pressupõe a existência do hardware, software e infra-estrutura necessários à utilização dos mesmos, onde se inclui o espaço físico, o fornecimento de energia eléctrica e de comunicações (dados e voz, locais e remotas), ventilação/aquecimento, iluminação, instalações sanitárias e dispositivos de controlo de acesso físico, podendo a contratação incluir ainda os recursos técnicos humanos necessários ao suporte dos sistemas a recuperar.

Em termos de alternativas estratégicas, a recuperação de sistemas poderá ocorrer noutras instalações da Empresa, em instalações de um fornecedor ou nas instalações de um parceiro de negócio, através de acordos de permuta de serviços, embora esta seja uma questão delicada, a abordar com precaução. Neste caso deverá considerar:

- que garantias de disponibilização dos recursos necessários à recuperação dos dados da sua Empresa lhe oferece um parceiro?
- essa recuperação implica interferência nas operações do seu parceiro? Se sim, que implicações poderão existir para a sua Empresa?
- quais as implicações se o seu parceiro também for atingido pelo desastre, mesmo que marginalmente?

A designação dada ao local onde é efectuada a recuperação dos sistemas está associada à disponibilidade do hardware e software e ao seu estado de prontidão. Desta forma temos os seguintes tipos de instalação:

Cold site Local onde apenas está disponível a infra-estrutura.

Warm site Local onde, para além da infra-estrutura, são disponibilizados os sistemas, que não se encontram preparados para entrar em funcionamento, sendo necessário proceder primeiro à instalação e configuração do software (sistemas operativos e aplicações) e, depois, à recuperação dos dados.

Hot site Local onde, para além da infra-estrutura, são disponibilizados os sistemas, que se encontram preparados para entrar em funcionamento, bastando para tal proceder à sua activação e/ou recuperação dos dados mais recentes, o que poderá ocorrer de forma praticamente instantânea no caso da utilização de algumas das tecnologias de armazenamento ou de cópia de segurança disponíveis.

A redução de custos pode ser conseguida através do sub-dimensionamento dos sistemas contratados nas instalações de recuperação, a troco da assunção de degradação do desempenho em caso de desastre, designando-se o modo de funcionamento resultante como "modo degradado". Por outras palavras, a Empresa assume que, em caso de desastre, o seu desempenho será inferior ao normal, mas nunca inferior ao necessário para o cabal cumprimento dos seus objectivos.

Adicionalmente, deverá ter-se em conta o clausulado preciso das licenças do software empregue, aproveitando, caso possível, o facto do software utilizado nas instalações de recuperação ser apenas activado aquando da indisponibilidade desse mesmo software no site afectado pelo desastre. Para além disso, a única altura em que as cópias do software serão utilizadas em simultâneo é no decurso de testes, o que poderá ser igualmente aceitável.

Idealmente, a transferência da utilização dos meios da Empresa para os do fornecedor, em caso de desastre, deverá ocorrer com o mínimo de impacto e de esforço. Se possível, as comunicações deverão ser redireccionadas de forma automática e transparente, tanto para o cliente como para as unidades não afectadas da Empresa. O grau de presença deste tipo de automatismos nos diversos planos, embora se deseje venha a ser elevado, pode ser outra forma de equilibrar eficientemente os custos na protecção contra desastres.

Exemplo: caso os equipamentos que ligam as redes locais de dados (LAN) das agências remotas à rede da Empresa (WAN) não suportem uma linha de comunicações alternativa para o centro de recuperação, existem diversas estratégias possíveis para ultrapassar esta limitação, com graus de automatismo e transparência distintos, tais como o *upgrade* ou a substituição dos equipamentos ou, com um menor custo, a introdução de equipamentos novos (de menor capacidade e ligados exclusivamente ao centro de recuperação) que, em caso de desastre, substituirão a actividade dos equipamentos existentes.

Plano de Contingência

O plano de contingência é composto pelos planos onde estão definidas as respostas iniciais (reflexas) a um incidente por parte de todas as áreas da Empresa, quer este ocorra com ou sem aviso prévio. Inclui todos os procedimentos de emergência, descrição das equipas que os executam, informação facilitadora da execução e indicação dos eventos que despoletam os procedimentos.

Exemplo: os incidentes associados a fenómenos meteorológicos ocorrem, muitas vezes, após aviso prévio. O Plano de Contingência da Empresa deverá contemplar os procedimentos de resposta aos alertas que a possam afectar.

Uma empresa cujas instalações sejam passíveis de sofrer inundação em caso de cheias num rio vizinho deverá incluir no seu Plano de Contingência um procedimento para a construção de muralhas de sacos de areia nos seus acessos mais sensíveis e para a transferência de equipamento passível de destruição por água para os pisos mais elevados. Este procedimento será activado em caso de alerta emitido pela Protecção Civil.

Estes planos deverão incluir procedimentos para todas as acções de emergência, incluindo:

- evacuação;
- primeiros socorros;
- redução de danos (por exemplo, extinção de fogo);
- contenção do incidente (por exemplo, desactivação de sistemas);
- avaliação de danos; e
- escalada e activação do plano de gestão de crise.

O plano de contingência deve descrever as equipas responsáveis pela execução de cada um destes procedimentos, indicando para cada equipa a sua designação oficial, constituição, estrutura hierárquica, a lista dos meios de que dispõe (diagramas, contactos, procedimentos, etc.) e planos de testes e exercícios, bem como de contactos para comunicação com outras equipas e centros de coordenação. Para além destes elementos, o plano de contingência deverá incluir um plano de acção composto por um diagrama de execução (ver Fig. IV-3) e uma matriz de responsabilidades que

permita identificar os procedimentos a usar, quem os executa e quando (ver exemplo da Fig. IV-4).

Para além dos elementos referidos, o plano de contingência deverá incluir todas as informações auxiliares que possam ser necessárias (como, por exemplo, contactos de serviços de emergência, de fornecedores contratados com cláusulas de suporte rápido, etc.). Para permitir a sua utilização pronta em caso de incidente, o plano deverá ser distribuído por todos os intervenientes e responsáveis, e ser guardado nas instalações a proteger, para que se encontre rapidamente acessível em qualquer eventualidade (mesmo em caso de falha de energia, por exemplo).

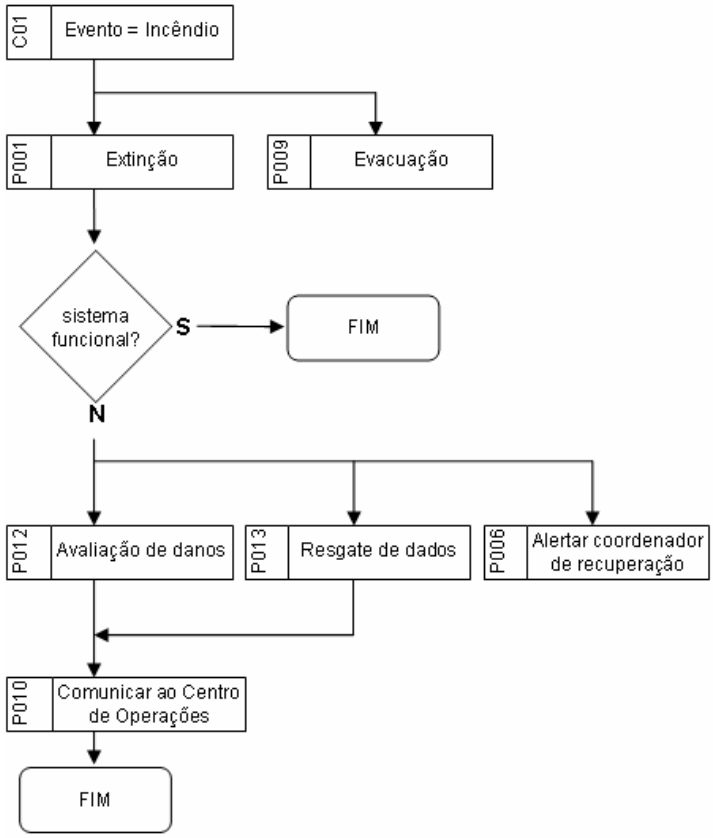


Fig. IV-3: Diagrama de execução – Exemplo

Matriz de Responsabilidades em Contingência

Incidente	Procedimento a executar	Responsável pela execução (extensão)	*Backup* do responsável (extensão)
Fogo	P001 – Procedimento em caso de incêndio	Guilherme Encarnação (1315)	João Santos (1121)
Inundação	P002 – Procedimento em caso de inundação	Diogo Oliveira (1261)	Ricardo Alves (1422)
Falha de Energia	P003 – Procedimento em caso de falha de energia	André Carvalho (1421)	José Silva (1392)
Tumulto	P004 – Procedimento em caso de tumulto	Gil Tavares (1132)	Sandra Nunes (1111)

Fig. IV-4: Matriz de Responsabilidades - Exemplo

Plano de Recuperação

O plano de recuperação é um documento composto pelas descrições das respostas a uma interrupção nas actividades, processos e funções importantes do negócio, que se prolongue para além das respectivas tolerâncias à indisponibilidade.

À semelhança do plano de contingência, para além dos procedimentos para cada processo e actividade críticos, o plano de recuperação deverá incluir a estrutura e constituição das equipas que os irão executar, o plano de acção e todas as informações auxiliares que facilitem a implementação dos procedimentos (por exemplo, contratos e listas de contactos), englobando a recuperação de:

- sistemas;
- dados;
- comunicações (de dados e de voz);
- processos TI e não tecnológicos (logística de matéria prima, etc.); e
- postos de trabalho.

Para além destes, deverão ser elaborados ainda procedimentos para o processo de comunicação externa (designada notificação), interna (designada de activação) e de declaração do desastre aos fornecedores de serviços de recuperação e de suporte (deslocação de pessoal e equipamento, apoio psicológico, etc.).

Ao definir os procedimentos do plano de recuperação deverá ser prestada uma grande atenção ao detalhe, de forma a garantir um sequenciamento em conformidade com os Tempos Alvo de Recuperação (TAR) dos processos e actividades críticos.

Finalmente, para garantir a sua sobrevivência ao desastre e a sua utilização pronta após um incidente, o plano deverá ser distribuído por todos os intervenientes e responsáveis, devendo ser guardadas cópias tanto nas instalações a proteger como fora delas[14].

Plano de Regresso à Normalidade

O plano de regresso à normalidade é um documento onde se definem os moldes como se irá processar a transição de instalações de recuperação de desastre para instalações definitivas.

---

[14] Existem casos reais de empresas que não conseguiram activar os seus planos de recuperação por estes terem sido destruídos no desastre que afectou a organização. Nenhum dos responsáveis possuía duplicados das cópias!

Este plano é composto pelos mesmos quatro elementos encontrados nos dois tipos de planos já apresentados, nomeadamente:

- um conjunto de procedimentos;
- a descrição das equipas que os irão executar;
- o plano de acção (baseado nas prioridades do negócio); e
- informações auxiliares.

No âmbito deste plano serão definidos os procedimentos de resgate de equipamentos (incluindo, se necessário, reparações) e instalações (obras), de aquisição de equipamento de substituição com carácter definitivo e de preparação das mudanças para as instalações definitivas. Deverá estar ainda prevista, dependendo das circunstâncias, a utilização de instalações temporárias, caso as definitivas não estejam disponíveis após o período contratado para as instalações de recuperação do fornecedor. Finalmente, também deverá ser produzida informação para declaração de sinistro junto das seguradoras.

Outra área de intervenção do plano de regresso à normalidade é a reconstituição de dados perdidos, que poderá ser conseguida, caso necessário, através de procedimentos de recuperação dos mesmos junto de terceiros (por exemplo, clientes e fornecedores).

A preservação de informações (através da sua anexação aos planos, etc.), tais como plantas, diagramas, contratos, contactos de fornecedores e outros, pode constituir um importante meio auxiliar do processo de recuperação de equipamentos e instalações.

Plano de Gestão de Crise

O plano de gestão de crise é activado por uma equipa de contingência que se depare com um desastre durante a execução do seu plano de contingência (ver Fig. IV-5). Este plano contém os elementos necessários à recuperação da capacidade de gestão durante

uma crise, permitindo à Empresa reter o controlo durante esse acontecimento.

Este plano é composto pela descrição da estrutura de comando e controlo da Empresa durante um desastre e pelo plano de comunicações, complementados com toda a informação auxiliar necessária (contratos, contactos de fornecedores, etc.).

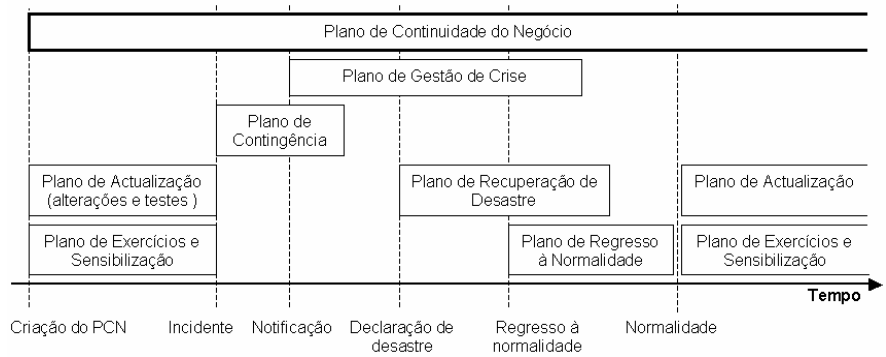


Fig. IV-5: Período de utilização dos planos constituintes do PCN

A estrutura de gestão de crise tem, tipicamente, equipas a três níveis (ver Fig. IV-6), que correspondem às capacidades de comando (decisão), controlo (coordenação) e operação (execução). O plano de gestão de crise implementa e articula estas equipas, através de procedimentos que descrevem o seu processo de activação, de formação, os papéis dos seus membros e o seu funcionamento, estipulando a base das operações, a sua constituição, os meios ao seu dispor (quadro, marcadores, folhas de papel, fotocopiadora, televisão, telefones, rádios, computadores portáteis, etc.) e as suas atribuições, incluindo a delegação de autoridade e os registos a fazer durante a crise (por exemplo, para posterior activação de seguros). É também na definição deste plano que se deverá prever o modo de autorização das despesas necessárias durante os períodos de contingência e recuperação do desastre.

O plano de comunicações deve contemplar os fluxos de transmissão de informação crítica sobre o desastre, incluindo os procedimentos de escalada (activação das equipas de gestão de crise) e

de declaração (comunicação com os parceiros), bem como árvores de contacto (cada elemento alerta um determinado número de colaboradores e assim por diante).

Para além destes procedimentos, este plano deve contemplar o processo de comunicação com o público (média/clientes), designado declaração, que deverá ser assente em técnicas de relações públicas. Nestas situações, para evitar especulação por parte dos média, a Empresa deverá assegurar a existência de um porta-voz que deve:

- estar por dentro da situação;
- responder a todas as perguntas;
- não mentir, confirmando o que é do conhecimento público bem como comunicando dados novos;
- estar suficientemente informado para saber responder a perguntas difíceis; e
- ser capaz de gerir a situação.

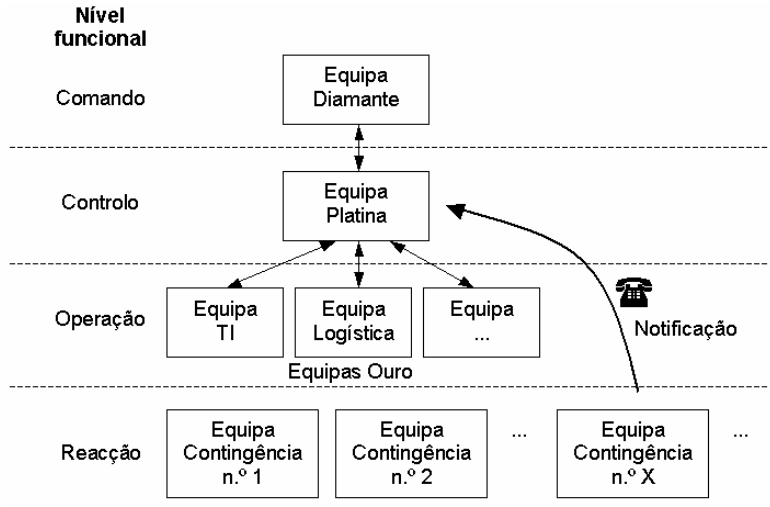


Fig. IV-6: Diagrama de articulação das equipas

Consoante a dimensão e actividade da Empresa poderá ser necessário contemplar também no plano de comunicação a criação de um centro de articulação com os familiares, que poderá, para além de facultar a informação mais actualizada aos familiares dos colaboradores, prestar apoio psicológico.

Implementação do Plano

Chegados à fase de implementação do plano de continuidade do negócio, irá proceder-se à integração dos meios necessários ao funcionamento dos procedimentos na Empresa e realizar o conjunto de medidas necessárias à divulgação do plano, ao seu teste e à nomeação das equipas.

Aquisição de Meios

O processo de aquisição dos meios necessários à concretização do plano de continuidade do negócio assenta na produção dos cadernos de encargos que servirão de base à consulta do mercado, após a qual as diferentes propostas apresentadas pelos vários fornecedores serão analisadas e comparadas, com vista à contratação.

Este processo é uma prática comum das empresas, pelo que a sua realização no âmbito do planeamento da continuidade do negócio apenas irá implicar algumas considerações, relacionadas com a particularidade do serviço ser solicitado ao fornecedor numa circunstância de desastre que, potencialmente, o poderá afectar também (por exemplo, num sismo). Esta particularidade implica, então, alguns cuidados na elaboração dos documentos de consulta, nomeadamente o requisito de acordos de níveis de serviço (tempos de resposta, etc.), com cláusulas de penalização por incumprimento, e da solicitação de garantias de sobrevivência a um desastre (através, por exemplo, da disponibilidade de centros noutras regiões).

No caso particular da contratação de instalações de recuperação, deverá ter-se em conta um conjunto de aspectos com impacto directo sobre a utilidade do serviço, como sejam a distância até às instalações a proteger, os meios de acesso, a quantidade e tipo de equipamento disponível, a infra-estrutura de suporte, o horário de funcionamento, o período durante o qual será disponibilizado o centro em caso de desastre e as garantias de segurança e confidencialidade. Não se deverá também esquecer a questão de como procederá o fornecedor na eventualidade de um desastre que afecte vários clientes seus: tem capacidade para todos em simultâneo? Que critérios de resposta utilizará?

Plano de Testes

A realização de testes visa garantir que os procedimentos contidos no plano de continuidade do negócio englobam todas as actividades necessárias à contingência, recuperação e retorno à normalidade da Empresa em caso de desastre, e que esses procedimentos funcionam correctamente. Pretende igualmente familiarizar os intervenientes com esses procedimentos, de modo a reduzir o número de decisões a tomar durante um desastre real, diminuindo a confusão, aumentando o controlo sobre a situação e diminuindo os custos do desastre. É este processo que permite que os intervenientes fiquem a conhecer a lógica de tomada de decisões durante um desastre, obrigatoriamente diferente de decisões tomadas em circunstâncias normais.

O plano de testes documenta:

- o processo de planeamento;
- o método de coordenação;
- o método de documentação;

- o processo de avaliação e comunicação dos resultados dos testes; bem como
- o método de introdução das alterações identificadas nos testes nos procedimentos.

O planeamento define o que irá ser testado, por quem, quando, com que finalidade e onde. Se possível, deverá incluir ainda um plano de contingência para o teste (prevendo, por exemplo, a indisponibilidade de um participante por doença).

A coordenação deverá garantir a correcta articulação das pessoas envolvidas, a gestão dos custos, a medição dos tempos (por exemplo, de recuperação) e o registo dos incidentes ocorridos no teste, bem como das alterações aos procedimentos, cuja necessidade se constate durante o teste.

O processo de documentação irá permitir o registo dos tempos observados, bem como das alterações necessárias aos procedimentos e as contribuições dos diversos participantes (fornecedor, utilizadores, etc.).

A avaliação deverá, sempre que possível, quantificar os resultados obtidos face aos Tempos Alvo de Recuperação identificados na análise de impacto no negócio. A comunicação dos resultados à Administração deverá descrever as áreas a melhorar e fornecer uma medida da capacidade de prontidão, bem como sugestões para a sua melhoria, sempre que necessário.

Por fim, o plano deverá detalhar uma metodologia para a introdução, no plano de continuidade do negócio, das alterações identificadas nos testes e para a validação dessas mesmas alterações.

O tipo de testes realizados deverá ser faseado, permitindo a evolução de exercícios mais simples e limitados, numa fase inicial, para testes mais completos e abrangentes numa fase posterior. Os tipos mais comuns são:

- ensaios gerais, com todas as equipas, em que os procedimentos são apenas lidos;

- testes modulares, realizados numa única área e focados numa única função; e
- testes funcionais, orientados para uma finalidade específica.

Todos estes tipos de testes podem ser realizados com ou sem pré-aviso. Nunca será demais realçar a importância da sua exaustividade e abrangência. Um plano, se não for testado, tem uma validade "teórica" que, em caso de necessidade de aplicação, poderá revelar-se desadequada às circunstâncias. Somente através da simulação de situações de crise se poderá aferir a qualidade das medidas planeadas, bem como o seu grau de sucesso.

Sensibilização e Formação

As actividades de sensibilização permitem assegurar a comunicação do plano de continuidade do negócio a todos os intervenientes, e colaboradores em geral, dando-lhes a conhecer:

- os componentes do plano;
- a importância da protecção contra o desastre;
- a identidade, função e contactos dos coordenadores das equipas;
- as formas de obterem informação (por exemplo, *web*, publicação interna, etc.);
- em que situações é activado o plano; e
- quais os testes que se irão realizar.

Para além da sensibilização, que se deverá estender a todos os colaboradores da Empresa, a execução dos procedimentos incluídos no plano de continuidade do negócio irá requerer actividades de formação específica dos intervenientes com responsabilidades, o que deverá ser também alvo de planeamento e orçamentação adequados.

Manutenção e Actualização

A manutenção e actualização do plano de continuidade do negócio requer o estabelecimento de um programa que suporte a sua comunicação periódica a todas as pessoas envolvidas, tanto para sensibilização como para o reforço da informação já anteriormente veiculada. Este programa deve, também, contemplar a realização do conjunto de actividades necessárias à introdução de alterações no plano, de modo a garantir permanentemente a capacidade de recuperação de um desastre.

Plano de Exercícios e Sensibilização

O plano de exercícios e sensibilização irá, simplesmente, repetir ao longo do tempo o processo de realização de testes e as actividades de sensibilização/formação já abordadas no âmbito da implementação do plano.

Plano de Actualização

O plano de actualização deverá implementar uma metodologia que permita a avaliação periódica da capacidade de recuperação e a introdução das alterações necessárias no plano de continuidade do negócio. Deverá igualmente promover a introdução no ciclo de vida de todos os projectos da Empresa de uma fase de avaliação do impacto desses mesmos projectos sobre o Plano de Continuidade do Negócio (PCN). Esta avaliação deverá, sempre que necessário, despoletar um processo de alteração ao plano.

Outro aspecto que deve estar previsto no plano de actualização é a reformulação das equipas em caso de saída de um dos seus membros da Empresa e a contextualização e formação dos recém-chegados.

O Plano de Actualizações deve prever a incorporação dos conhecimentos adquiridos durante a reacção a um desastre (as lições aprendidas) e deverá também prever medidas para evitar a repetição de eventuais erros que tenham sido cometidos ou acidentes que tenham ocorrido na aplicação prática dos planos.

Conclusão

A reacção face a um desastre é sempre algo de imprevisível e de consequências muitas vezes incalculáveis. O modo como a Empresa reage a estes eventos determina a sua capacidade de sobrevivência, mas demonstra igualmente o tipo de preparação e de atenção prévia que dedicou a esta questão. A criação de um plano de reacção a desastres, com todas as suas componentes, não é uma tarefa linear e requer a participação empenhada de todos os escalões da organização. Se bem que possa parecer uma tarefa inglória, devido ao enorme esforço associado e à sua fraca visibilidade, a criação de medidas de segurança face ao desastre será um garante da viabilidade da organização caso o pior se concretize.

Capítulo V - Padrões e Legislação

Não é objectivo dos autores, com este capítulo, analisar detalhadamente todas as questões legais relacionadas com os sistemas de informação – para tal existem outros títulos no mercado, escritos por especialistas. Contudo, este livro ficaria incompleto sem uma referência a alguma legislação nacional e ao grande padrão internacional que se ocupa desta matéria.

A nível legislativo, em Portugal tem-se assistido a um esforço, relativamente recente, de criação de peças legais que visam enquadrar as novas tecnologias e as actividades por elas suportadas. O próprio Estado tem tentado dar o exemplo através de uma série de orientações que obrigam os serviços públicos a ter presença na Internet (presença esta avaliada periodicamente), bem como através de várias iniciativas enquadradas juridicamente.

Este capítulo pretende, então, dar a conhecer algumas das leis nacionais relacionadas com as novas tecnologias, que os autores consideram mais pertinentes. Para além disso, olharemos para o ISO/IEC 17799, o standard internacional dedicado à segurança da informação e que é de leitura obrigatória para qualquer responsável pela segurança da informação empresarial.

Legislação nacional

De um modo geral, em Portugal não se tem acompanhado com muita atenção os aspectos legais da informática, sendo grande parte da nossa legislação neste campo transposições de directivas comunitárias e esforços avulsos de regulamentação. Esta “falta de actividade legislativa” pode traduzir a adequabilidade das leis já existentes mas pode, também, significar a necessidade de um

esforço de actualização legislativa nacional, face às novas realidades do século XXI.

Porém, a partir da quinta revisão constitucional, de 2001, a Lei Fundamental da República passou a garantir livre acesso às redes informáticas de uso público e a proibir o tratamento de dados pessoais que violem os direitos, liberdades e garantias e que propiciem a discriminação, o que se pode interpretar como sendo um sinal claro da tomada de consciência da importância exercida pelas novas tecnologias na sociedade.

Segurança Nacional

A peça legislativa que talvez se possa considerar o ponto de partida dos esforços reguladores subsequentes nesta área remonta a 1990 (28 de Fevereiro) e traduz-se numa Resolução do Conselho de Ministros (Resolução n.º 5/90), que aprova as "Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática", mais conhecida por SEGNAC 4.

Este diploma tenta abarcar todas as áreas da segurança informática, desde as características físicas dos centros de processamento de dados, passando pela definição de cópias de segurança, até à destruição segura de suportes informáticos. Se bem que se dedique essencialmente a sistemas que processem, armazenem ou transmitam dados classificados, não deixa de possuir interesse para o responsável pela segurança, uma vez que contém princípios válidos para implementações mais seguras.

Para além disso, pode servir de ponto de partida para uma abordagem mais estruturada de uma descrição pormenorizada da política de segurança da organização: este diploma contém, senão todos, pelo menos a maioria dos tópicos que deverão constar de um documento de orientação empresarial.

Criminalidade Informática

Remonta a 1991 a lei que categoriza e pune os ilícitos criminais na área da informática. A Lei n.º 109/91, de 17 de Agosto, respondendo às necessidades sentidas à época, vem, então, definir seis categorias de crimes informáticos, puníveis por lei com penas que podem ir de multas, passando por prisão, até ao encerramento definitivo de estabelecimentos. De notar que as tentativas de concretização dos ilícitos definidos nesta lei também são punidas.

As categorias de crimes informáticos em vigor em Portugal são:

- **Falsidade informática**: introdução, alteração ou eliminação ilegítimas de dados ou programas informáticos que possam servir de meios de prova em relações jurídicas (com a intenção de produzir "documentos" falsos);
- **Dano relativo a dados ou programas informáticos**: introdução, alteração ou eliminação ilegítimas de dados ou programas informáticos com o objectivo de causar prejuízos a terceiros ou proveitos próprios;
- **Sabotagem informática**: introdução, alteração, eliminação ou interferência ilegítimas em dados, programas ou sistemas informáticos, com o objectivo de perturbar (ou interromper) o seu funcionamento ou a sua transmissão;
- **Acesso ilegítimo**: acesso ilegítimo a um sistema ou rede informática;
- **Intercepção ilegítima**: intercepção não autorizada de comunicações num sistema ou rede informática;
- **Reprodução ilegítima de programa protegido**: reprodução, divulgação ou comunicação pública não autorizadas de um programa informático protegido por lei[15].

---

[15] De notar que esta protecção é definida pelo Código do Direito de Autor e dos Direitos Conexos.

Devido à sua definição suficientemente genérica, estas categorias abarcam a quase totalidade das actividades criminais informáticas e são utilizadas na investigação e punição de ilícitos criminais.

O responsável pela segurança deverá, tanto na elaboração da política e normas de segurança da organização como na implementação de soluções técnicas de protecção, ter em mente estas definições e o modo como elas podem influenciar as suas decisões.

Exemplo: se existir a intenção de instalar um *sniffer* na rede empresarial, como forma de registar todo o tráfego existente, esta opção poderá ter implicações, se não for devidamente enquadrada: para todos os efeitos, a instalação de software que registe toda a actividade de uma rede de comunicação de dados pode ser entendida como "intercepção ilegítima". Neste exemplo, o melhor será procurar o conselho do departamento jurídico da organização e determinar se, caso se opte por uma solução destas, os utilizadores não terão de ser devidamente informados. Por outro lado, neste caso, também deverão ser tidos em linha de conta os pareceres da Comissão Nacional de Protecção de Dados, entidade a abordar mais adiante.

Como nota final, relativamente à criminalidade informática, importa referir que Portugal é um dos 47 países signatários da Convenção sobre Cibercrime, assinada a 23 de Novembro de 2001 em Budapeste. O objectivo desta Convenção, uma vez ratificada pelos signatários, é o de harmonizar as legislações nacionais relativas a crimes informáticos (incluindo conteúdos ilegais tais como pornografia infantil ou violações de *copyright* entre outros), adoptar medidas (legais e outras) para a investigação de crimes informáticos e promover a cooperação internacional no campo investigativo, o que inclui a possibilidade de extradição de infractores. No tratado da convenção prevêem-se igualmente medidas para a monitorização, fiscalização, apreensão, armazenamento, etc., de dados das investigações (ou resultantes destas).

Protecção de Dados Pessoais

Em 1998 dá-se a transposição para a ordem jurídica portuguesa de uma directiva comunitária relativa à protecção dos dados pessoais. O diploma daí resultante, Lei n.º 67/98, de 26 de Outubro[16], vem regulamentar a forma como devem ser tratados os dados pessoais das pessoas singulares, bem como a sua transmissão.

A preocupação essencial desta lei é a protecção dos direitos, liberdades e garantias fundamentais dos cidadãos: ao longo dos seus 52 artigos, a Lei 67/98 aborda os diferentes tipos de bases de dados, de acordo com os seus conteúdos, estabelecendo, sempre que necessário, medidas específicas para o seu tratamento, e atribuindo responsabilidades por quaisquer más práticas detectadas.

Parecem-nos de particular significado as disposições relativas à segurança, que trazem, inquestionavelmente, implicações para as empresas que possuam bases de dados, por exemplo de clientes. Dada a sua relevância, citemos aqui o Número 1 do Artigo 14º: "O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger."

Da leitura deste excerto sobressaem, imediatamente, dois aspectos essenciais: qualquer base de dados deve ser protegida por medidas técnicas e organizativas (i.e., não basta instalar soluções técnicas, mas são necessários procedimentos e orientações claras) e essa protecção deve ser adequada aos riscos existentes, o que implica o

---

[16] Com a Declaração Rectificativa n.º 22/98, de 28 de Novembro.

conhecimento por parte do responsável (pelo tratamento) de quais os riscos que podem afectar adversamente os dados, quer sejam externos, quer internos. Nestes últimos, incluem-se potenciais erros dos operadores das bases de dados, pelo que, nalguns casos, pode ser necessária a implementação de mecanismos de verificação e autenticação dos dados existentes.

A entidade que supervisiona o cumprimento desta lei é a Comissão Nacional de Protecção de Dados, uma entidade bastante activa e que abordaremos mais adiante. É junto desta entidade que todas as bases de dados contendo informação de cariz pessoal têm, obrigatoriamente, de ser registadas.

Ainda sobre este tema, resta referir que existe igualmente legislação que regulamenta a recolha, processamento e transmissão de dados pessoais relacionados com as telecomunicações, o que, dependendo da área de actividade da organização, pode ser pertinente[17].

Comércio Electrónico

Foi preciso chegar a 1998 para que Portugal assumisse a importância do comércio electrónico e o tentasse enquadrar legalmente. Este esforço foi oficialmente iniciado pela Resolução de Conselho de Ministros n.º 94/99, de 25 de Agosto, que cria a Iniciativa Nacional para o Comércio Electrónico e define os seus objectivos no campo da legislação, da sensibilização e da promoção. A partir deste momento, assistiu-se a um esforço de enquadramento de vários actos electrónicos com vista ao seu reconhecimento como elementos válidos de transacções comerciais.

Neste sentido foram aprovados o decreto-lei n.º 290-D/99, de 2 de Agosto, que define o regime jurídico dos documentos electrónicos e

---

[17] Ver Lei n.º 69/98, de 28 de Outubro ("Regula o tratamento dos dados pessoais e a protecção da privacidade no sector das telecomunicações [...]"), revogada pela Directiva 2002/58, de 12 de Julho.

da assinatura digital, e o decreto-lei n.º 375/99, de 18 de Setembro, que equipara a factura electrónica à factura de papel[18]. Também se pode interpretar como fazendo parte deste esforço a transposição para a lei nacional (decreto-lei n.º 58/00 de 18 de Abril), da Directiva Comunitária n.º 98/48/CE, que "(...) estabelece os procedimentos administrativos a que obedece a troca de informação (...) [relativa] aos serviços da sociedade de informação (...)".

Por fim, uma referência à Directiva 2000/31/CE, de 8 de Junho, justamente intitulada "Directiva sobre o comércio electrónico", que regulamenta alguns aspectos legais relacionados com os serviços da sociedade da informação (contratos electrónicos internacionais, colaboração entre Estados-membros, resolução de litígios, acções judiciais, entre outros)[19].

Todos estes diplomas têm como objectivo criar as bases sobre as quais se possam construir relações comerciais, electrónicas, juridicamente válidas. Contudo, um elemento essencial deste esforço é o reconhecimento das partes e a não repudiação dos contratos firmados, razão pela qual se desenvolveram leis no campo das assinaturas digitais.

Assinaturas Digitais

O já citado decreto-lei n.º 290-D/99, resultante da Iniciativa Nacional para o Comércio Electrónico, para além de equiparar um documento electrónico a um documento de papel, vai mais longe, introduzindo a validade das assinaturas digitais e a sua força probatória, i.e., o seu valor como prova.

---

[18] Ver, também, o Decreto Regulamentar n.º 16/00, de 2 de Outubro, que define as condições e requisitos de utilização da factura, ou documento equivalente, transmitidos por via electrónica.

[19] Nesta Directiva, no seu Artigo 7º, surge o direito ao registo de opção negativa (*opt-out*) para comunicações comerciais não solicitadas (conhecidas como *spam*).

Consciente da permanente evolução tecnológica, o legislador tentou fazer com que este diploma fosse ágil, antecipando a sua possível aplicação a "(...) outras modalidades de assinatura electrónica que satisfaçam os requisitos de segurança da assinatura digital".

Assim, um documento electrónico, desde que devidamente assinado com uma "assinatura digital certificada por uma entidade credenciada" passa a ter o mesmo valor que um documento de papel devidamente assinado, o que significa que as empresas podem realizar negócios por via electrónica, com a validade de contratos "físicos", de papel.

Caso a assinatura electrónica não seja certificada por uma entidade oficial, o valor do documento submete-se aos termos gerais do direito. Portanto, para que haja validade oficialmente reconhecida, torna-se necessário obter um certificado digital junto de uma entidade reconhecida. Em Portugal, e como já vimos no capítulo "Áreas da Segurança Empresarial" deste livro, no capítulo dedicado à *Public Key Infrastructure* (PKI), a autoridade credenciadora é o Instituto das Tecnologias da Informação na Justiça, assistido pelo Conselho Técnico de Credenciação[20]. Este instituto, através de uma unidade intitulada "Gabinete de Credenciação, Auditoria e Segurança", tem como incumbência "assegurar o completo exercício das funções de entidade credenciadora". Esta definição, como facilmente se percebe, é suficientemente vaga para não nos esclarecer sobre quais são, precisamente, os requisitos para o reconhecimento das entidades emissoras de certificados digitais. Mas, independentemente desta circunstância, já existem em Portugal várias empresas dedicadas, em exclusividade ou não, à emissão de certificados digitais. Ou seja, já é possível realizar transacções oficiais através de meios electrónicos.

---

[20] O Conselho Técnico de Credenciação, constituído por cinco elementos, é um órgão consultivo que emite pareceres ou recomendações relativamente às entidades certificadoras reconhecidas (criado pelo decreto-lei n.º 234/2000, de 25 de Setembro).

Existe ainda um aspecto que merece realce no decreto-lei em análise e que se prende com a presunção de que, a partir do momento em que um documento electrónico é digitalmente assinado, foi o titular (ou representante autorizado) da assinatura a apô-la no documento, com a intenção de o assinar. Mais, a lei ainda presume que o documento não é alterado desde a aposição da assinatura.

Se este último aspecto se consegue garantir através de mecanismos de chave pública/chave privada (já abordados neste livro), as duas outras questões merecem alguma reflexão. Com as actuais fragilidades existentes nos sistemas e redes informáticos, não será difícil imaginar cenários em que alguém assina, sem o saber, um documento digital, ou em que um intruso acede ao sistema onde se encontra o certificado e o utiliza ilegitimamente.

Estes aspectos sublinham a importância de, ao aderir aos certificados digitais "oficiais", serem criadas medidas de segurança adequadas para evitar a sua utilização não autorizada.

Licenciamento de Software

Atendendo a que o software, como qualquer outra criação industrial, não se refere, em termos legais, unicamente à sua área exclusiva, a lista de legislação que controla a sua utilização, fundamentalmente em termos de protecção contra cópias, é extensa.

Dela fazem parte o Código do Direito de Autor e dos Direitos Conexos (Lei n.º 114/91), o Regime de Protecção Jurídica dos Programas de Computador (Lei n.º 252/94) e a Lei n.º 122/00, relativa à Protecção Jurídica das Bases de Dados, entre outros. Como também vimos, a própria lei da Criminalidade Informática prevê a reprodução ilegítima de programa protegido como crime passível de punição.

É por este motivo que o controlo das existências, em termos de software, nas empresas assume uma particular importância. De um modo geral, a regra aplicável é a de "um programa – uma licença",

sendo que, obviamente, existem diversas modalidades de licenciamento, com encargos diferenciados.

Mais do que conhecer a legislação aplicável, importa reconhecer a premência da legalização, e controlo, dos programas em uso na Empresa. Para tal, podem ser adoptadas várias medidas, técnicas e processuais, que visem garantir o cumprimento, não só da lei, mas da própria política interna da organização. Podem, por exemplo, ser previstas sanções, reflectidas na política da Empresa, para os colaboradores que instalem software não autorizado nos sistemas informáticos.

Por outro lado, o recurso a soluções técnicas para impedir a proliferação de "cópias piratas" pode igualmente ser considerado: existem produtos no mercado que inventariam as existências, em termos de software, dos sistemas ligados em rede, outros que centralizam e controlam a distribuição e instalação de programas ou, mais simplesmente, existe a possibilidade de criação de políticas, ao nível da infra-estrutura da organização, que limitem e condicionem a adição de componentes novos de software.

Comissão Nacional de Protecção de Dados

A Lei de Protecção de Dados Pessoais, já anteriormente abordada, menciona, no seu Capítulo IV e seguintes, uma organização com poderes para verificar o cabal cumprimento da lei. Essa organização, a Comissão Nacional de Protecção de Dados (CNPD), funciona junto da Assembleia da República e detém um vasto leque de competências, desde a emissão de pareceres até à deliberação sobre a aplicação de coimas, podendo a sua actividade verificadora ser accionada mediante denúncias ou queixas de particulares[21].

---

[21] A Lei n.º 68/98, de 26 de Outubro, atribui mesmo à CNPD as funções de instância nacional de controlo junto da instância comunitária de controlo que cria um serviço europeu de polícia (EUROPOL).

Ainda de acordo com a lei, todas as entidades públicas e privadas têm a obrigação de colaborar com a CNPD, facultando-lhe acesso a todas as informações necessárias, incluindo, claro está, aos conteúdos de bases de dados.

Os poderes desta comissão são bastante latos, podendo inclusivamente, para além das punições legais que podem ir de coimas a penas de prisão, obrigar as organizações a eliminar registos existentes nos seus sistemas ou mesmo bases de dados inteiras. As suas decisões são, segundo a lei, obrigatórias (se bem que passíveis de recurso).

A CNPD é uma entidade bastante activa: uma rápida leitura dos seus relatórios anuais revela um número significativo de intervenções, quer de autorização, quer de fiscalização, bem como de emissão de pareceres sobre os mais variados aspectos. De facto, se à primeira vista a actividade desta comissão se encontra "limitada" pela Lei n.º 67/98, uma análise mais atenta do seu articulado revelará um campo de acção bastante alargado.

Ao incidir sobre a protecção de dados pessoais, a referida lei abre as portas a um elevado número de áreas, sobre as quais a CNPD terá uma palavra a dizer: a privacidade nos locais de trabalho, as questões de avaliação de crédito e de solvabilidade, o tratamento de decisões de tribunais, são apenas alguns exemplos de temas abordados por este organismo, resultantes em orientações públicas[22].

A consulta do seu sítio na Internet (http://www.cnpd.pt) é uma actividade obrigatória para qualquer responsável pela segurança de qualquer organização, uma vez que, através da leitura das orientações emanadas, poderá obter valiosíssimos instrumentos de adequação da política, normas e procedimentos internos que pretenda implementar, ou que já existam.

---

[22] Uma medida de segurança física que carece igualmente de registo junto da CNPD é a utilização de câmaras de vídeo-vigilância.

O Standard ISO/IEC 17799

A norma ISO/IEC 17799 é um standard internacional dedicado à segurança da informação, reconhecido pela sua abrangência e que contém diversas orientações, mais ou menos complexas, que visam contribuir para a definição e manutenção de um determinado nível de segurança das organizações, dos seus colaboradores, instalações e sistemas de informação. O próprio título deste standard permite ter uma ideia do seu objectivo: "Tecnologias da Informação – Código de prática para a gestão da segurança da informação".

O ISO/IEC 17799 está organizado em dez capítulos, que visam cobrir diferentes tópicos ou áreas da segurança:

1. Política de Segurança;
2. Segurança Organizacional;
3. Controlo e Classificação de Bens;
4. Segurança do Pessoal;
5. Segurança Física e Ambiental;
6. Gestão das Comunicações e das Operações;
7. Controlo de Acessos;
8. Desenvolvimento e Manutenção de Sistemas;
9. Gestão da Continuidade do Negócio;
10. Conformidade.

Cada um destes capítulos pormenoriza, no seu interior, os vários aspectos relacionados com o respectivo tema, sugerindo medidas que visam possibilitar a obtenção do nível de segurança pretendido pelo standard. De facto, a leitura deste documento deverá ser realizada à luz das reais necessidades da organização, pois as sugestões que ele preconiza apontam para níveis de segurança extremamente elevados, os quais, se contrastados com as caracterísi-

cas das organizações, poderão ser descabidos ou, mesmo, impossíveis de atingir.

Este standard visa, então, transmitir abordagens comuns para a resolução dos diversos aspectos de segurança por ele tratado. Se, por um lado, este documento pode ser encarado como um ponto de partida para a implementação da segurança da informação, por outro poderá revelar a carência de medidas específicas para cumprir os requisitos de algumas empresas. O seu objectivo declarado é, afinal, o de fornecer uma base comum para o desenvolvimento de padrões de gestão da segurança empresarial.

A sua consulta constitui, em resumo, uma leitura obrigatória para o responsável pela segurança da Empresa.

Certificação

A certificação por esta norma não é tarefa fácil, pois devido à sua abrangência e à latitude dos seus requisitos, possui implicações na organização como um todo. Atendendo a este grau de complexidade, existem diversos sítios na Internet que fornecem informação detalhada e até algum software, que pode ser adquirido, e que visa guiar o utilizador pelos diversos passos básicos para estabelecer um nível de segurança na organização, compatível com os pré-requisitos do ISO/IEC 17799.

A análise de risco é um requisito básico desta norma, sendo referido ao longo de todo o documento, pois é apenas através desta análise que será possível identificar o nível de segurança actual da organização e os passos necessários para garantir um nível de segurança aceitável. As etapas definidas pela organização deverão então ser consistentes com os requisitos da norma, de modo a garantir que se está a caminhar no sentido da certificação, ou pelo menos no sentido de uma melhora significativa da segurança da Empresa (ver capítulo “Gestão do Risco”).

Garantir a adequação da segurança da informação aos níveis pretendidos, definindo e implementando planos de acção que permi-

tam, de forma abrangente, ter uma organização segura não é tarefa fácil; porém, cada vez mais se torna uma tarefa necessária, dada a complexidade das organizações, a quantidade de informação recolhida e a facilidade de acesso e partilha dessa mesma informação.

A certificação pretende, fundamentalmente, demonstrar e garantir que a Empresa tem assegurados níveis de segurança básicos. Contudo, mesmo que a Empresa não opte pela certificação, as dez áreas referidas no ISO/IEC 17799 são um bom começo para uma análise cuidada e abrangente da segurança da organização: onde nos encontramos e para onde caminhamos.

Conclusão

O corpo legislativo existente, como vimos, apesar de poder não acompanhar permanentemente a evolução da tecnologia, consegue, regra geral, responder às necessidades mais prementes em termos de regulamentação e orientação política, de mercado, etc. Com os esforços reguladores da Comunidade Europeia, e a transposição das suas directivas para a ordem interna dos Estados-membros, é de prever que esta situação venha a sofrer alterações a curto/médio prazo, atendendo às exigências de um mercado comum cada vez mais apoiado nas novas tecnologias.

Perante esta realidade, o enquadramento legal dos esforços empresariais, nomeadamente na área da segurança, deve ser encarado como uma necessidade carente de acompanhamento por parte de especialistas. Desta forma, recomenda-se que, na elaboração do Programa de Segurança, o seu responsável recorra ao apoio do departamento jurídico, ou de peritos nesta área, como forma de garantir o cumprimento dos requisitos legais aplicáveis.

Esperamos, contudo, que a abordagem que aqui foi realizada a um núcleo da legislação existente nesta área, possa servir de referência aos conteúdos mais pertinentes, lançando alguma luz sobre o seu conteúdo.

Capítulo VI - Criação do Plano de Segurança

O Programa de Segurança é o processo que visa elevar a segurança da Empresa para o nível requerido pela mesma através da introdução de medidas que permitam reduzir a exposição a todos os riscos presentes para um nível definido. Este processo implica a aceitação de determinados riscos (reduzidos ou de impacto inferior ao custo das medidas necessárias à sua redução), a transferência de outros riscos (por exemplo, através da contratação de um seguro) e a redução dos riscos cuja probabilidade de ocorrência e/ou impacto estejam acima do limite definido.

Para garantir que este programa se encontra de acordo com os objectivos do negócio é necessário identificar antecipadamente o nível de segurança pretendido pela Administração. Uma vez definido o nível alvo, é chegada a hora de definir a estratégia para levar a segurança à Empresa, estratégia essa que deverá reflectir os princípios apresentados anteriormente (ver “Princípios de Prevenção e Protecção”, no capítulo “Teoria da Segurança”) e os objectivos do negócio, de uma forma que permaneça inalterada enquanto a própria estratégia do negócio o permanecer.

Após a definição da estratégia é necessário identificar e analisar os riscos existentes (ver “Gestão do Risco”) e determinar as diversas acções de prevenção e protecção que poderão diminuir esses riscos, prioritizando-as segundo a estratégia escolhida.

Neste capítulo serão listados e descritos os principais componentes do Plano Global de Segurança, bem como as respectivas metodologias de definição e factores de sucesso na sua promoção junto da Administração da Empresa.

Os Documentos da Segurança

A segurança empresarial é norteada por um conjunto de documentos que conferem consistência e exequibilidade às medidas implementadas. Estes documentos são:

- o Plano Global de Segurança;
- a Política de Segurança;
- as Normas de Segurança; e
- os Procedimentos.

Iremos ver, de seguida, qual o conteúdo e função de cada um destes documentos.

Plano Global de Segurança

O Plano Global de Segurança é o documento principal da segurança na Empresa. É neste documento que se irá encontrar a análise de risco da Empresa, a estratégia e o plano de acção para a implementação das medidas.

O conteúdo deste documento será analisado posteriormente em detalhe em “Componentes do Plano Global de Segurança”.

Política de Segurança

A Política de Segurança é um conjunto reduzido de regras que definem, em linhas gerais, o que é considerado pela Empresa como aceitável ou inaceitável, contendo ainda referências às medidas a impor aos infractores. Esta Política deverá referenciar todas as outras políticas existentes na Empresa que contenham regras de segurança, bem como fazer alusão às Normas de segurança, descritas adiante.

As regras contidas neste documento devem ser suficientemente genéricas para não necessitarem de revisão, excepto em caso de alteração profunda do contexto do negócio (por exemplo, mudança de ramo de actividade).

Exemplo: Toda a informação armazenada, transmitida ou processada pelos sistemas de informação da <Empresa> é propriedade dessa empresa.

Podem-se encontrar milhares de exemplos de Políticas de Segurança com uma simples pesquisa na Internet, bem como de políticas específicas de:

- acesso remoto;
- uso aceitável do acesso à Internet;
- uso aceitável do correio-electrónico;
- ligação à rede;
- etc.

Para permitir a utilização rigorosa das políticas, as regras incluídas deverão ser numeradas e cada política deve indicar a versão da sua redacção.

A Política de Segurança deve ser do conhecimento de todos os colaboradores da Empresa, possivelmente através da edição de um folheto, que deverá ser fornecido aos colaboradores no decurso do seu processo de admissão.

Normas de Segurança

As Normas de Segurança são o documento composto por todas as regras de segurança da Empresa, concretizando em detalhe as linhas orientadoras estabelecidas na Política de Segurança. É neste documento que deverão estar referenciadas as tecnologias utilizadas na Empresa e a forma segura de as utilizar.

Apesar do grau de detalhe pretendido ser superior ao encontrado na Política de Segurança, as Normas não deverão conter detalhes de implementação ou operação, o que confere ao documento alguma intemporalidade. Desta forma, não é aconselhável referenciar nas Normas de Segurança aspectos relativos a marcas, modelos ou versões, algo que deverá ser deixado para o nível mais baixo da documentação de segurança: os procedimentos.

Exemplo: Os sistemas operativos deverão, sempre que tal seja possível, ser configurados por forma a impedir a instalação de software pelos utilizadores.

Procedimentos

Um procedimento é um documento que descreve uma operação de forma muito detalhada, ou seja, indicando todos os seus passos. Este tipo de documentos poderá sofrer alterações frequentes e, tipicamente, não é escrito unicamente por causa da segurança, pelo que deverá ser feito um trabalho de sensibilização junto dos técnicos da Empresa no sentido de que estes garantam a conformidade dos procedimentos por eles escritos com as Normas de Segurança.

Componentes do Plano Global de Segurança

Tal como já referido, este é o documento principal da segurança na Empresa, descrevendo os objectivos do Programa de Segurança, a forma da sua implementação e as razões para a sua realização.

Os principais elementos constituintes do Plano Global de Segurança são:

- os objectivos do Programa de Segurança;
- a situação actual da segurança na Empresa;
- a estratégia;
- o plano de acção;

- os benefícios decorrentes do plano de acção;
- a estrutura funcional (descrição dos papéis dos diversos membros da equipa de segurança);
- o orçamento e os recursos necessários;
- a terminologia técnica utilizada.

Para facilitar a sua leitura por executivos de topo, o Plano Global de Segurança deverá incluir no seu início um sumário executivo, contendo um resumo sintético do documento, com os principais valores e conclusões existentes, bem como referências aos números das páginas onde o leitor poderá obter informação adicional sobre cada elemento referido no sumário.

Neste sub-capítulo iremos abordar os elementos do Plano Global de Segurança a montante da definição do plano de acção, sendo os elementos que o suportam abordados nos sub-capítulos seguintes.

Objectivos

A definição do Plano Global de Segurança deve iniciar-se com a determinação dos objectivos a atingir pelo Programa de Segurança da Empresa. Estes objectivos deverão ser perenes, sendo a alma do Programa de Segurança e o compromisso assumido pelo seu responsável, reflectindo ainda a postura da Administração em matérias de segurança.

Exemplo: "O Plano Global de Segurança visa garantir a protecção das pessoas, informação e instalações contra as ameaças quotidianas, bem como a continuidade do negócio da <Empresa> face a desastres de impacto regional ou mais reduzido."

Uma vez que o Programa de Segurança visa elevar o nível de segurança da Empresa para o nível requerido pela mesma, é importante que estes objectivos estabeleçam esse nível, preferencialmente de forma assente em métricas baseadas em padrões (ver "Acordos de

Nível de Serviço"). Essas métricas deverão permitir aferir o grau de cumprimento dos objectivos, ou o enquadramento nos mesmos das medidas propostas no âmbito do Plano Global de Segurança.

Análise de risco

Para que a Administração aprove um conjunto equilibrado e completo de objectivos será necessário avaliar a situação actual da segurança na Empresa, realizando uma análise de risco. A inclusão desta análise no Plano Global de Segurança visa sensibilizar a Administração, por forma a obter o seu apoio, aumentando a confiança no equilíbrio e adequação do Programa de Segurança, através da justificação das medidas propostas resultantes da classificação dos riscos.

A análise de risco realizada no âmbito do Plano Global de Segurança poderá basear-se numa das metodologias apresentadas anteriormente, em "Gestão do Risco", sendo necessário incluir no plano a descrição do modelo utilizado na quantificação, bem como os dados recolhidos e as conclusões produzidas. Para facilitar a consulta do documento pela hierarquia deverá ser apresentada uma síntese da análise de forma preferencialmente gráfica.

Estratégia

Aprovados os objectivos, o responsável pela segurança deverá definir uma estratégia para os atingir. Esta abordagem deverá identificar as grandes linhas de actuação, que deverão manter-se, no essencial, inalteradas no decorrer dos anos seguintes. Para tal, deverá evitar referenciar tecnologias, ou outros elementos operacionais, cuja alteração não se reflicta no macro-contexto.

Exemplo: "No âmbito do Programa de Segurança, a <Empresa> irá implementar uma infra-estrutura de segurança capaz de proteger os sistemas de informação, elevando anualmente o grau de maturidade da segurança

> e implementando uma estrutura de recolha de dados capaz de permitir determinar a identidade e metodologia dos atacantes."

A estratégia definida deverá reflectir os princípios apresentados anteriormente em "Princípios de Prevenção e Protecção" e os objectivos estratégicos do negócio intimamente ligados à segurança.

Plano de Acção

O plano de acção é o componente do Plano Global de Segurança que transpõe para a prática a estratégia definida, detalhando as actividades que serão realizadas num determinado período.

Este plano é composto pelo macro-planeamento das actividades (lista de actividades e calendário), pelo orçamento, pela lista dos recursos humanos e materiais necessários e pela discriminação dos benefícios esperados pela implementação de cada uma das actividades.

Uma vez que a criação de planos de acção se insere num contexto mais alargado do que o da segurança, não iremos alongar-nos sobre este tema, embora seja importante referir a utilidade de assentar o plano proposto numa análise de custo/benefício (ver "Estratégia de Controlo" no capítulo "Gestão do Risco").

Como Vender Segurança à Administração

Um documento sem utilidade não tem valor, pelo que a definição do Plano Global de Segurança só termina com a sua aprovação. Neste capítulo iremos debruçar-nos sobre este processo, que medeia a definição e a implementação, sendo esta última abordada mais adiante, no capítulo "Gestão do Programa de Segurança".

Os Papéis da Administração e do Responsável pela Segurança

A Administração da empresa é quem define a estratégia do negócio e que escolhe as iniciativas a realizar para a sua implementação. Desta forma, é a este corpo administrativo que compete decidir ao mais alto nível as actividades que se irão realizar na empresa, sendo a função do responsável pela segurança dotar a Administração da informação necessária para que esta possa optar.

A comunicação com o mais alto nível decisório depende do posicionamento hierárquico do responsável pela segurança, da sua visibilidade no interior da organização e da postura da sua hierarquia directa. Em algumas situações será este responsável a dirigir-se directamente à Administração da empresa e, noutras, poderá estar na dependência de um superior hierárquico que assumirá essa atribuição. Independentemente do posicionamento do responsável pela segurança, o contacto com a Administração será necessário para obter orçamento e para garantir o apoio ao mais alto nível em medidas de carácter transversal, que se estendam fora do âmbito técnico dos sistemas de informação, entrando pelos domínios do Negócio, tais como a definição de políticas de segurança.

A interacção com a Administração é necessária tanto para a sensibilizar relativamente à necessidade de empreender uma determinada actividade, como para a apresentação e justificação de propostas e sua posterior aprovação, ou ainda para demonstrar o sucesso e a necessidade de desenvolvimento das mesmas. Nestes contactos é necessário utilizar uma linguagem não técnica, por forma a facilitar a transmissão da mensagem que se pretende fazer passar.

Linguagem e Enquadramento

Para obter aprovação para uma iniciativa, o responsável pela segurança necessita, primeiramente, de conseguir justificá-la à Adminis-

tração. Para tal, terá necessariamente de lhe conseguir fazer chegar uma mensagem não deturpada, o que implica a utilização de linguagem adequada e de rigor, como forma de conseguir transmitir a informação pretendida e, deste modo, conseguir alcançar os objectivos propostos. Será importante, também, notar que é necessário muni-la de informação de gestão em detrimento de opiniões, uma vez que estas últimas não são justificáveis.

Uma vez que a segurança dos sistemas de informação e o Negócio são áreas de conhecimento distintas, existe a tendência para os especialistas destes domínios não terem conhecimentos significativos do outro. Desta forma, existe algum desconhecimento do Negócio por parte dos especialistas dos sistemas de informação, sendo o inverso igualmente verdadeiro. A maneira tradicional do responsável pela segurança dos sistemas de informação ultrapassar esta barreira é através da utilização de estatísticas imediatas de cariz mediático, empregando uma linguagem simples ao alcance de todos. Esta utilização algo abusiva de estatísticas acarreta alguns problemas. Mark Twain, o escritor e jornalista americano, dizia haver três tipos de mentiras: as mentiras, as malditas mentiras e as estatísticas. Na segurança, as estatísticas podem revelar-se uma forma de mentira, insensibilizando a médio/longo prazo a Administração, através da habituação desta a cenários apocalípticos que não se concretizam. A razão desta afirmação prende-se com o contexto das estatísticas apresentadas ser frequentemente errado para o uso que é feito das mesmas. O enquadramento adequado é de extrema importância ao fornecer este tipo de dados à Administração como fundamento dos pedidos. O que muitos outros fazem ou declaram, nem sempre é adequado à nossa situação particular e específica. Um exemplo clássico é a utilização generalizada das estatísticas das pesquisas realizadas anualmente pelo CSI[23] nos

[23] O Computer Security Institute é uma organização norte-americana de referência, fundada em 1974, dedicada à segurança dos computadores e redes, sendo responsável pela realização de importantes conferências

EUA. Os dados recolhidos nesta pesquisa são extremamente interessantes para os profissionais da segurança e não só, detalhando o cenário de ataques e atacantes com números recolhidos de forma científica e rigorosa. O único problema é que esse estudo é realizado nos EUA, dificilmente um termo de comparação com uma empresa da Baixa Lisboeta, de Faro, ou de outra região, especialmente se tivermos em conta a sua dimensão (apenas 7% das empresas consultadas no estudo têm menos de 1.000 funcionários).

A utilização incorrecta de estatísticas deve-se apenas em parte a descuido, ocorrendo maioritariamente devido à inexistência das fontes equivalentes em território nacional. Os gestores, naturalmente, não aceitam com facilidade dados cujo contexto não seja o seu e poderão não se dar ao trabalho de separar uns números "maus" dos restantes indicadores, descartando o pacote na sua totalidade, pelo que é preciso ter cuidado com as estatísticas. Desta forma, será necessário dar visibilidade a incidentes reais, ocorridos no seio da empresa, podendo-se para tal proceder à recolha desta informação através da realização de pilotos de detecção de intrusão, de filtragem de conteúdos em *gateway*, da monitorização de acesso físico, ou de outras tecnologias de detecção. A estes dados deverá ser anexada a informação dos sistemas existentes, tal como a análise dos dados recolhidos pelos sistemas antivírus.

Uma forma de justificar o investimento em segurança é através da recolha de informação relativa à concretização de ataques. Após a recolha de informação sobre ameaças concretizadas, registadas na nossa empresa, é de extrema importância dedicar tempo à preparação de relatórios informativos, contendo informação sobre as intrusões e acidentes registados, desde os vírus às assinaturas de ataque, à qual poderemos adicionar dados relativos à observação de incidentes de segurança relatados pela concorrência. Também estes relatórios informativos devem ser redigidos na óptica do

---

nesta área e que, em conjunto com o FBI, conduz anualmente um inquérito sobre segurança informática a milhares de empresas nos EUA.

negócio, utilizando uma linguagem adequada à transmissão aos destinatários, nas áreas de negócio, da informação crítica neles contida. Estes elementos deverão servir de suporte às propostas apresentadas à Administração, uma vez integradas na análise de risco subjacente às actividades do Plano Global de Segurança.

A informação facultada à Administração deverá ser veiculada na linguagem do negócio, sendo sintetizada a partir dos dados de detecção, da informação sobre os ataques e da análise de risco realizada a partir destes elementos. A título de exemplo, poder-se-iam cruzar os dados sobre o número de vírus detectados e as características desses vírus para determinar o impacto financeiro sobre a Empresa num determinado período. Mediante esta informação, a Administração estará habilitada a tomar decisões.

Independentemente da forma de comunicação empregue, o sucesso da interacção entre o responsável pela segurança e a Administração mede-se pela taxa de aprovação das medidas apresentadas a esta última, ditando não só os meios que estarão ao dispor da área de segurança, bem como a força de que se irão revestir as suas iniciativas.

Obrigações Legais

Os riscos legais podem justificar a adopção de medidas que, de outra forma, não seriam facilmente justificadas. Apesar da letra da Lei parecer à primeira vista preto-no-branco, uma breve conversa com um advogado rapidamente tornará claro que o mundo é feito de cinzentos, não devendo assumir-se que todas as leis são para cumprir a qualquer custo.

Cabe ao responsável pela segurança o dever de veicular à Administração as obrigações legais da Empresa (ver “Padrões e Legislação”) que representem riscos e de incluir no plano de actividades do Plano Global de Segurança as medidas para a redução desses riscos, baseadas numa análise de custo/benefício.

Cenários Alternativos

Raramente (se é que alguma vez) um problema de gestão terá uma solução única, pelo que a apresentação de diversos cenários é uma forma de controlar o desfecho de um processo de validação administrativo em que a solução proposta pelo responsável pela segurança seja preterida, devido ao seu impacto financeiro ou por outra razão. Estes processos, que podem ter um desfecho imprevisível e potencialmente negativo para a segurança, com a validação de soluções ad-hoc com "bom aspecto" mas desequilibradas, podem ser controlados capitalizando o posicionamento do responsável pela segurança como especialista na matéria, através da apresentação de alternativas nos diversos pontos do espectro económico, processual ou de outro carácter.

Em matéria de segurança, os cenários típicos correspondem à aceitação, redução, controlo ou transferência do risco, cenários esses que deverão ser preparados e documentados na sua relação custo/benefício pelo responsável pela segurança, permitindo à Administração a tomada de uma decisão informada, com base nas diversas alternativas propostas. Naturalmente, por uma questão de eficiência, só se deverá incorrer no esforço necessário à elaboração dos diversos cenários alternativos em matérias mais complexas ou problemáticas, ou que impliquem o dispêndio de somas significativas.

Exemplo: considere os seguintes quatro cenários simples para resolução do problema de infecções virais nos computadores da Empresa.

1) aceitação do risco:	incorrendo em prejuízos da ordem estimada.
2) controlo do risco:	incorrendo nos custos do sistema antivírus e economizando o valor dos prejuízos da ordem estimada.

3) redução do risco: limitando as comunicações autorizadas associadas a vectores de propagação viral (por exemplo, impedindo o acesso a determinados conteúdos *Web* ou à execução de determinados anexos a mensagens de correio electrónico), incorrendo em parte dos prejuízos da ordem estimada e incorrendo nos custos de configuração generalizada dos sistemas.

4) transferência do risco: optando por utilizar caixas de correio-electrónico num fornecedor externo, a quem é atribuída a obrigação de detectar vírus, incorrendo nos custos do serviço (beneficiando das economias de escala realizadas pelo ISP) e economizando o valor dos prejuízos da ordem estimada.

Equipa de segurança

A segurança eficaz requer a uniformização dos critérios de classificação e das medidas de redução dos riscos, algo que se pode entender como a necessidade de dotar a Empresa com um pensamento global de segurança. Para tal é necessário que a segurança

seja materializada como uma responsabilidade associada a um indivíduo, ou equipa de indivíduos, caso a dimensão e estrutura da Empresa assim o justifique.

Neste capítulo iremos analisar diversos aspectos da equipa responsável pela segurança na Empresa, aspectos esses que se manterão inalterados quer a responsabilidade da segurança seja repartida entre os responsáveis de diversas outras áreas quer sobre um ou mais indivíduos afectos exclusivamente à segurança.

Antes de avançar, porém, é importante referir que, apesar da realidade nacional ainda não revelar muitas empresas com responsáveis em segurança dedicados, esse é o caminho que se antevê no momento. Este sentimento é reforçado quotidianamente pelo ciclo de violência registado pelo Mundo, com a escalada do terrorismo iniciada em 11 de Setembro de 2001.

Dimensão

A segurança não é um produto mas sim um processo contínuo, que existe tanto ao nível estratégico, como táctico e operacional. Da definição e respectivos requisitos para implementação e gestão das medidas de segurança contempladas, irá resultar o dimensionamento da equipa que as irá realizar.

Existem basicamente três modalidades de afectação de recursos à segurança: em dedicação exclusiva ou em dedicação parcial, com ou sem responsabilidade global. Apesar da primeira destas modalidades não se encontrar ao alcance de muitas empresas, especialmente das PME, esta é a forma mais eficiente de levar a segurança ao seu negócio.

Não existe uma fórmula para calcular o número de colaboradores da Empresa que deverão estar afectos à segurança. No entanto, existem três factores que deverão ser considerados.

O primeiro factor é a relação entre o negócio/Empresa e o risco. Quanto maiores os riscos a que o negócio e a Empresa estão

sujeitos, maior atenção deverá ser prestada à segurança, atenção essa que se deverá reflectir no número e perfil dos elementos afectos à equipa, bem como no orçamento ao seu dispor.

Exemplo: pequenas empresas de pesquisa laboratorial, cujas fórmulas ou produtos sejam extremamente valiosos.

A complexidade da Empresa é o segundo elemento a ter em conta no dimensionamento da equipa de segurança. Neste aspecto, quanto maior o número de colaboradores ou o número de processos, por exemplo, maior a necessidade de afectar recursos à prevenção e protecção.

Exemplo: empresas com grande dispersão geográfica.

Por fim, no dimensionamento da equipa de segurança deverá ter-se em conta o modelo de confiança existente e aquele que é pretendido, e considerar os recursos necessários à gestão dessa mudança.

Exemplo: empresas com uma percentagem muito significativa de pessoal temporário.

Responsabilidades

O responsável pela segurança tem como incumbência a criação e gestão do Programa de Segurança da Empresa. Para tanto terá a responsabilidade de criar, promover e gerir o Plano Global de Segurança, tendo para tal de efectuar uma análise de risco capaz de identificar os principais riscos, bem como definir as estratégias de prevenção e de protecção.

No âmbito das actividades do Plano Global de Segurança, o responsável deverá escrever, validar e promover políticas e normas de segurança, sensibilizar e formar a hierarquia, restantes colaboradores e terceiros, bem como envolver-se de raiz em projectos novos.

Por fim, compete ao responsável pela segurança da Empresa ser o interlocutor interno em matérias de segurança, servindo de consultor e de conselheiro.

Enquadramento

O enquadramento do responsável e da sua eventual equipa de segurança na estrutura da Empresa reflecte-se sobre a sua capacidade, alcance e força no interior da mesma.

Existem duas formas principais de posicionamento para esta função: num departamento transversal ou no interior de uma área técnica (tipicamente nos sistemas de informação). Cada uma destas formas tem as suas vantagens e desvantagens, como veremos de seguida.

Comecemos por abordar as situações em que a hierarquia da empresa entende a função de responsável pela segurança como estando enquadrada num departamento transversal. Este enquadramento tem a vantagem de conferir isenção e independência à função da segurança, conferindo-lhe uma maior visão sobre a Empresa e visibilidade na mesma, o que é um forte catalisador positivo, tanto para as acções de sensibilização, como para o bom andamento da validação das políticas e normas de segurança. O principal inconveniente deste tipo de enquadramento é o afastamento da realidade da Empresa que poderá ocorrer se o responsável pela segurança ou a sua equipa não estiverem dotados das *social skills* necessárias.

O outro posicionamento frequentemente encontrado para a função de segurança, que consiste na inserção da segurança no interior de uma área técnica, visa reduzir o alheamento da realidade que se pode produzir com o enquadramento descrito anteriormente. Infelizmente, na prática, a proximidade de uns resulta frequentemente no distanciamento de todos os outros, levando à perda da visão transversal da Empresa e à consequente introdução de medidas de segurança desproporcionadas, predominantemente oriundas da

área onde a função se encontra enquadrada. Um exemplo clássico é a integração da função de segurança na área de redes, de onde quase sempre resultam medidas de segurança fortemente tecnológicas. Na realidade, a tecnologia não é a "pílula dourada" milagrosa, apesar de frequentemente as medidas tecnológicas implementadas assim o sugerirem.

Exemplo: colocando a um técnico a questão do comprimento e complexidade da palavra-passe mínima de rede, entre (suponhamos) a obrigatoriedade de um comprimento mínimo de 6 caracteres independentemente da sua natureza e a obrigatoriedade de utilização de uma palavra-passe mínima com 8 caracteres, que inclua números, símbolos e letras, este poderá optar pela segunda. Apesar desta solução parecer adequada do ponto de vista do técnico, considerando um ponto de vista mais abrangente que englobe a população dos utilizadores da Empresa, podemos concluir, no entanto, que tal medida pode resultar num decréscimo do nível real de segurança, uma vez que uma parte dos utilizadores, que não conseguiria gerir mentalmente uma palavra-passe tão complexa, a iria apontar num papel, que manteria acessível, colada no monitor ou debaixo do teclado.

Perfil

Quais são as principais características necessárias ao bom desempenho da função de segurança?

Em primeiro lugar devemos considerar as duas componentes distintas do Programa de Segurança: a criação e gestão do programa e a Administração no dia-a-dia das medidas que este implementa. Se, por um lado, é necessário um especialista em segurança para a definição e gestão do Programa de Segurança da empresa, por outro lado, para a Administração no dia-a-dia (tipicamente técnica)

bastará um especialista na tecnologia ou matéria relevante. Por exemplo, ao definir um sistema de controlo de acesso deverá o responsável pela implementação ficar responsável pela gestão do sistema? Consoante a dimensão da empresa e da sua infra-estrutura, assim poderão ou não ser transferidos estes processos para peritos que irão fazer a operação diária dos mesmos, libertando o especialista em segurança.

Pelo carácter transversal da segurança, o seu responsável deverá não só ser um gestor competente, mas também ter conhecimentos técnicos significativos nas diversas áreas descritas anteriormente em "Áreas da Segurança Empresarial", conhecimentos esses que deverão estender-se para além das tecnologias e plataformas.

Para além destas características de cariz técnico, o responsável deverá ainda possuir uma elevada capacidade de comunicação, aliada a uma grande curiosidade, persistência, rigor e perfeccionismo, para além de ser metódico. Para complementar estes traços de personalidade, deverá ainda ser flexível e capaz de procurar e estabelecer compromissos. Tudo isto, no entanto, não servirá de muito sem formação específica em segurança, algo que no passado era difícil de conseguir na Europa, fora do âmbito técnico (aplicações, tecnologias, sistemas, etc.)

Orçamento

O orçamento necessário à implementação de um Programa de Segurança na Empresa irá depender fortemente do tipo de negócio e da sua exposição ao risco, bem como do seu parque tecnológico e do percurso a realizar em matéria de segurança (diferença entre o nível actual no modelo de maturidade e o nível pretendido). Como linha orientadora, no planeamento do Plano Global de Segurança, pode considerar-se um orçamento para a segurança na ordem dos 5% do orçamento dos sistemas de informação.

Acordos de Nível de Serviço

Uma metodologia possível para a implementação do Plano Global de Segurança passa pela inclusão de serviços de segurança no processo de definição de acordos de serviço, sendo necessário para tal contemplar ainda a implementação de uma infra-estrutura de suporte a estes serviços.

Estes acordos são contratos, internos ou com terceiros, estabelecidos entre um proprietário de informação e o responsável pela prestação do serviço que a disponibiliza, que visam limitar o âmbito e nível dessa prestação, possivelmente através da associação de um custo.

Uma parte importante dos acordos é, precisamente, o acordo de nível de serviço (ou SLA - *Service Level Agreement*), que discrimina os serviços a prestar no âmbito do acordo e os moldes em que serão prestados.

Como iremos ver em seguida, os SLA podem assentar na classificação da informação como meio de garantir uma definição equilibrada, conferindo um nível de protecção e prevenção similares à informação com sensibilidade equivalente.

Classificação da Informação

No capítulo do acordo de serviço sobre segurança deverá constar a classificação dos requisitos de confidencialidade, de integridade e de disponibilidade da informação. Essa classificação deverá ser feita pelo proprietário da informação segundo critérios uniformes, comuns a todos os acordos de serviço estabelecidos.

A classificação da confidencialidade da informação deve reflectir os danos para a Empresa decorrentes da divulgação indevida dessa informação. Esses danos deverão ser estimados, qualitativa ou quantitativamente, pelo proprietário da informação.

A tabela seguinte mostra um exemplo possível de graus de classificação dos requisitos de confidencialidade.

Grau	Designação	Danos decorrentes da divulgação não autorizada
1	Pública	Nenhuns
2	Interna	Danos insignificantes
3	Confidencial	Danos razoáveis
4	Muito Secreto	Danos muito significativos ou desastrosos

Fig. VI-1: Classificação dos requisitos de confidencialidade

À semelhança da classificação da confidencialidade, a definição do requisito de integridade da informação armazenada e processada irá reflectir os danos para a Empresa decorrentes da corrupção irrecuperável, parcial ou total, desta informação. Tal como referido na confidencialidade, esses danos deverão ser estimados, qualitativa ou quantitativamente, pelo proprietário da informação.

A tabela seguinte mostra um exemplo possível de graus de classificação dos requisitos de integridade.

Grau	Designação	Danos decorrentes da corrupção dos dados
1	Nulo	Nenhuns
2	Mínimo	Danos insignificantes
3	Médio	Danos razoáveis
4	Elevado	Danos muito significativos ou desastrosos

Fig. VI-2: Classificação dos requisitos de integridade

Da mesma forma que o proprietário da informação procedeu à classificação da confidencialidade e requisitos de integridade dessa informação, ele deverá classificar o seu requisito de disponibilidade, reflectindo nessa classificação as consequências para a Empresa decorrentes da indisponibilidade dessa informação em função do tempo. Tal como nos casos anteriores, estas consequências podem ser estimadas de forma qualitativa ou quantitativa.

A tabela seguinte mostra um exemplo possível de graus de classificação dos requisitos de disponibilidade.

Grau	Designação	**Duração total da indisponibilidade tolerada por mês**
1	Muito Baixa	Inferior a uma semana
2	Baixa	Inferior a 2 dias
3	Média	Inferior a 7 horas
4	Elevada	Inferior a uma hora
5	Permanente	Não são tolerados períodos de indisponibilidade

Fig. VI-3: Classificação dos requisitos de disponibilidade

Serviços de Segurança

Num acordo de serviços podem ser disponibilizados serviços em praticamente todas as áreas da segurança referidas anteriormente em “Áreas da Segurança Empresarial”.

A título de exemplo, num acordo poderão estar presentes os seguintes serviços:

- Área: segurança lógica
  - impermeabilização do S.O.
  - impermeabilização aplicacional
  - controlo de acessos
  - protecção antivírus
  - detecção de intrusão
  - medidas de dissimulação
  - cópia de segurança de dados (*backup*)
- Área: segurança física
  - controlo de acessos
  - protecção de suportes de cópia
- Área: protecção de desastre
  - criação e manutenção do Plano de Contingência
  - criação e manutenção do Plano de Continuidade do Negócio

Estes serviços poderão ser detalhados em maior ou menor grau em função da maturidade da prestação de serviços, podendo-se incluir serviços com maior especificidade. No exemplo anterior, tal especificação adicional poderia reflectir-se da seguinte forma sobre o serviço de controlo de acessos da segurança lógica:

- Área: segurança lógica
  - Controlo de Acessos
    - acesso ao sistema operativo
    - acesso remoto
      - através da Intranet
      - através de outra *Extranet*

  - através da Internet
  - através de rede privada virtual (VPN)
  - por modem
- acesso aplicacional

Tal como o exemplo acima exposto, os restantes serviços também poderão ser detalhados em função da infra-estrutura de segurança disponibilizada.

Critérios de Disponibilização

Os serviços de segurança a prestar, no âmbito de um acordo, deverão ter por base de referência a classificação realizada pelo cliente, quer esta seja efectuada nos moldes descritos anteriormente, quer em quaisquer outros que se escolha. Esta classificação deverá nortear o cliente na selecção das opções de serviço contratadas, garantindo a consistência dessa modalidade com a natureza da informação que será disponibilizada.

Exemplo: o cliente não deverá poder optar por um *backup* semanal para uma informação classificada com um requisito "elevado" de integridade, nem prescindir de antivírus num sistema de suporte a informação classificada "secreto" em termos de confidencialidade.

Pelo exposto deverá depreender-se que os serviços facultados em matérias de segurança deverão ser disponibilizados ao cliente com limites que podem ser representados numa matriz, tal como o exemplo da tabela seguinte.

Nível do serviço	Prazo para concluir a acção requerida	Classificação permitida												
		Confidencialidade				Integridade				Disponibilidade				
		1	2	3	4	1	2	3	4	1	2	3	4	5
Muito Baixo	**Um mês**		X	X	X			X	X					
Baixo	**Duas semanas**			X	X				X					
Médio	**Uma semana**				X									
Elevado	**Três dias**													
Permanente	**24 horas**													

Serviço disponível X Serviço indisponível

Fig. VI-4: Matriz de disponibilidade de um serviço - Exemplo

Exemplo: considerando a tabela da Fig. VI-4, se o cliente tiver classificado o requisito de confidencialidade da informação com grau 4, então não poderá contratar o serviço de nível “médio”.

Tabelas similares poderão ser criadas e usadas para cada serviço de segurança, por forma a permitir ao cliente do acordo escolher o nível desejado de acordo com a sensibilidade da informação.

Conclusão

Neste capítulo foi analisada a primeira fase do Programa de Segurança, que consiste na sua definição, materializada no Plano Global de Segurança, e foi abordado o problema da complexa articulação

do Responsável pela segurança com a Administração da Empresa, necessária à conclusão deste processo.

Em seguida serão abordadas as restantes fases do programa, em que este será implementado e gerido.

Capítulo VII - Gestão do Programa de Segurança

Após a definição, aprovação e implementação do Programa de Segurança empresarial, o seu responsável terá de o gerir, o que poderá eventualmente incluir a administração da respectiva infra-estrutura (dos sistemas), consoante a dimensão da equipa a ele afecta.

Neste capítulo iremos abordar os problemas associados à gestão deste programa, desde a recolha de informação de gestão, passando pelo *reporting*, pelo controlo e pela avaliação.

Pretendemos chamar a atenção do leitor para alguns dos factores críticos de sucesso do Programa de Segurança, como é o caso de um planeamento bem efectuado, um controlo eficaz, fluxos de comunicação eficientes e a correcta gestão da mudança, entre outros.

O Programa de Segurança, pela sua abrangência e complexidade, deverá ter uma gestão eficaz e atenta, uma supervisão forte, e deverá, acima de tudo, envolver a Empresa como um todo. Se assim for, e os factores críticos de sucesso forem devidamente acautelados, conseguiremos um programa eficiente, capaz de atingir com sucesso os objectivos predefinidos.

Controlo de Gestão

O desempenho de uma Empresa depende de diversos factores, sendo apenas alguns dos quais controláveis. Alterações inesperadas no meio envolvente, por exemplo, são elementos fora do controlo da organização, logo, factores que não são reflectidos de forma antecipada no seu planeamento. A Empresa deve, então,

controlar o desempenho dos seus colaboradores de forma a reconhecer quais as causas do seu sucesso organizacional que resultam do planeamento, dos objectivos e da análise do meio envolvente, e quais resultam de factores inesperados.

A necessidade de controlar é proporcional à dimensão da Empresa, ou seja, quanto maior e mais complexa a organização, maior a necessidade de efectuar um controlo apertado da sua evolução, tentando detectar eventuais desvios e respectivas causas.

A complexidade do Programa de Segurança é crescente, devido à necessidade de acompanhamento do progresso da Empresa e, também, da evolução das tecnologias e do meio ambiente como um todo. Torna-se, assim, essencial garantir que o Programa de Segurança é correctamente definido, e que todos os factores aprovados são devidamente executados, tanto em termos de prazos como de resultados.

O modo como é efectuado o controlo de gestão na Empresa pode variar segundo um modelo mais clássico ou mais actual, mais simples ou mais complexo mas, independentemente do modelo utilizado, teremos certamente como base uma premissa fundamental: somente podemos controlar aquilo que previmos, orçamentámos e planeámos, o que implica que, para tal controlo, deve existir um ponto de partida, uma base que indique se agimos de acordo com o planeado ou se ocorreram desvios e, neste caso, de que natureza (desvios de orçamento, de prazos, de recursos, etc.).

Metodologias de Controlo de Gestão

As metodologias de controlo de gestão, como já afirmado, vão das mais simples, como a mera criação de um orçamento, às mais complexas, como é o caso dos *balanced scorecards*.

Diferentes organizações usam metodologias distintas. Contudo, todas elas visam efectuar o acompanhamento, quer seja de projectos, de programas ou da evolução da Empresa como um todo.

O ponto de partida para o controlo de gestão será sempre, em qualquer dos casos, a definição de objectivos, ou seja, de onde se pretende chegar, bem como das implicações deste processo, isto é, dos custos em que a incorrer, do dispêndio de tempo, recursos a afectar, etc. Todos estes elementos visam identificar o ponto de partida para o controlo, na medida em que tentam prever o que esperamos que aconteça, permitindo verificar posteriormente o que correu mal, o que correu bem, e quais as razões para os diversos desvios. Permitindo evitar no futuro alguns desses erros agora cometidos.

Como metodologias mais utilizadas, poderemos referir as seguintes:

- o orçamento simples;
- o orçamento flexível; e
- os *balanced scorecards*.

Em seguida iremos abordar cada uma destas metodologias.

Orçamento Simples

A primeira das metodologias de controlo de gestão apresentadas consiste na definição, no início do período económico em análise, de um orçamento: uma previsão do que se espera gastar para atingir determinado objectivo e do que se espera receber em retorno (vendas, benefícios, etc.). No final desse período verifica-se se os objectivos foram ou não atingidos, após o que é efectuada uma análise dos desvios.

O orçamento simples é caracterizado pelo seu alto nível, isto é, em termos da Empresa indica pouco mais do que as vendas e os custos de diversos elementos (ver Fig. VII-1).

Quando se trata de um projecto de dimensões pequenas ou médias esta metodologia é a mais utilizada, sendo apenas apresentados os custos a incorrer em diversas categorias: consultoria, hardware,

consumíveis, horas extra, etc. Trata-se de informação básica, mas suficiente para efectuar uma análise de alto nível aos desvios detectados. É um orçamento que, pelas suas características, é efectuado em pouco tempo e, no caso de projectos de orçamento reduzido e de pequena dimensão, é plenamente suficiente, tendo em conta o custo/benefício de um orçamento mais detalhado e o tempo adicional necessário à sua elaboração.

ARTIGO	VALOR
Consumíveis	€ 9.600
Hardware	€ 33.600
Software	€ 16.700
Recursos Humanos	€ 121.500
TOTAL	**€ 181.400**

Fig. VII-1: Orçamento Simples – Exemplo

Orçamento Flexível

À medida que se evolui para uma metodologia de orçamento flexível, o orçamento vai sendo mais detalhado, permitindo efectuar, à posteriori, análises mais aprofundadas aos desvios encontrados.

Este documento inclui não só as premissas e conclusões, mas também os elementos adicionais que espelham o raciocínio que as relaciona. Ao elaborar este tipo de orçamento, será necessário, então, especificar as diversas rubricas na base da sua construção. Desta forma, ao encontrar um desvio nas conclusões, o orçamento flexível inclui detalhe suficiente para se apurar quais as premissas correspondentes a essas conclusões as responsáveis pelo desvio.

O orçamento flexível permite analisar se um determinado desvio foi provocado por um erro resultante das quantidades definidas (devido a falhas de análise ou improdutividade) ou se é devido a diferenças não antecipadas (por exemplo, nos preços dos produtos adquiridos).

Exemplo: supondo que é prevista a aquisição de 100 *tapes* para efectuar *backups* ao longo do ano, a um custo total de € 5.000, e que, no final do ano, o custo das *tapes* registado foi de € 7.500, um orçamento flexível permitirá identificar se esse desvio se deveu a um aumento do preço estimado das *tapes* ou a um acréscimo da quantidade de *tapes* adquiridas e, neste último caso, se tal se ficou a dever a um erro de cálculo, ou a uma falha de optimização dos *backups*.

Trata-se de um orçamento mais detalhado, que implica um maior consumo de tempo na sua elaboração, mas que permite efectuar uma análise mais pormenorizada dos desvios e das suas causas (ver Fig. VII-2).

Este tipo de documento será à partida o mais indicado no caso de projectos de maior dimensão, ou com maior orçamento, como é normalmente o caso do Programa de Segurança.

ARTIGO	VALOR	VAL. UNIT.	QUANTIDADE
Consumíveis			
• papel	€ 2.500	2	1250
• tinteiros	€ 1.500	30	50
• *toner*	€ 3.000	30	100
• suportes magnéticos:			
o CDs	€ 500	100	5
o disquetes	€ 100	20	5
o *tapes*	€ 2.000	50	40
Sub-total:	**€ 9.600**		
Hardware			
• monitores	€ 4.500	30	150
• CPUs	€ 9.000	9	1000
• computadores portáteis	€ 6.000	4	1500
• impressoras	€ 11.300	10	1130
• fotocopiadoras (manutenção)	€ 1	2800	2800
Sub-total:	**€ 33.600**		
Software			
• produto A	€ 6.500	6500	1
• produto B	€ 7.200	7200	1
• produto C (*upgrade*)	€ 3.000	3000	1
Sub-total:	**€ 16.700**		
Recursos Humanos			
• internos	€ 30.000	1500	20

ARTIGO	VALOR	VAL. UNIT.	QUANTIDADE
• externos	€ 90.000	6000	15
• deslocações	€ 1.500	150	10
Sub-total:	**€ 121.500**		
TOTAL	**€ 181.400**		

Fig. VII-2: Orçamento Flexível - Exemplo

Balanced Scorecard

A metodologia *balanced scorecard* assenta em indicadores que representam os principais eixos de interesse da Empresa, com base nos quais é efectuada a avaliação dos resultados. Esta metodologia tem vindo a ganhar popularidade junto das organizações e, apesar de ser complexa e morosa, especialmente na fase de implementação, tem como vantagem permitir avaliar o desempenho da organização de uma forma integrada com a sua estratégia.

Segundo esta metodologia, são definidos indicadores, sendo atribuído um peso a cada por forma a perfazer 100%. Estes variam de acordo com os eixos de interesse de cada Empresa, podendo ser, por exemplo, indicadores de vendas, ou de formação dos colaboradores, sendo acima de tudo indicadores congruentes com a estratégia e partilhados por toda a organização.

Os *balanced scorecards*, para além de serem uma metodologia de controlo, são um novo marco da gestão estratégica das organizações, reflectindo a estratégia da Empresa, constituindo-se como um processo de aprendizagem, dado permitirem a comunicação da

estratégia a todos os colaboradores, reflectindo ao longo do tempo as variações fundamentais da Empresa.

A necessidade de implementação de um Programa de Segurança e a dotação de recursos e orçamento ao mesmo, com vista à obtenção de um patamar de segurança considerado necessário, deverá também ser reflectida pela introdução dos objectivos deste programa no *balanced scorecard*, reflectindo as suas preocupações com a segurança.

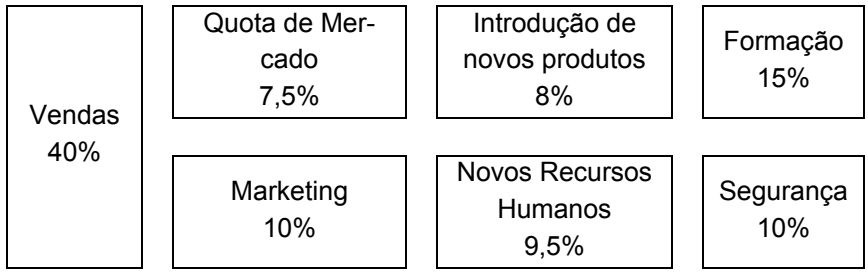


Fig. VII-3: Balanced Scorecard - Exemplo

Como visto, o controlo de gestão pode ter por base diversas metodologias, sempre com o objectivo de avaliar o desempenho da Empresa, identificando o que é resultado do desempenho dos seus colaboradores e o que se deve a factores inesperados do meio envolvente.

Avaliação de Desempenho

Algumas organizações avaliam os seus programas e departamentos com base em indicadores financeiros, como sejam a relação entre o resultado operacional e o investimento (ou *Return on Investment* - ROI), ou o valor actual líquido (VAL), que corresponde à actualização de *cash flows* futuros esperados, ou então a avaliação dos resultados finais e sua comparação com o orçamento e objectivos inicialmente propostos. Em qualquer dos casos, deverá ser prestada especial atenção à determinação das causas dos desvios, sem procurar imputar culpas aos gestores por factores fora do seu controlo.

Fases da Gestão de Programas

As diversas fases do Programa de Segurança são caracterizadas pelos objectivos indicados na Fig. VII-4.

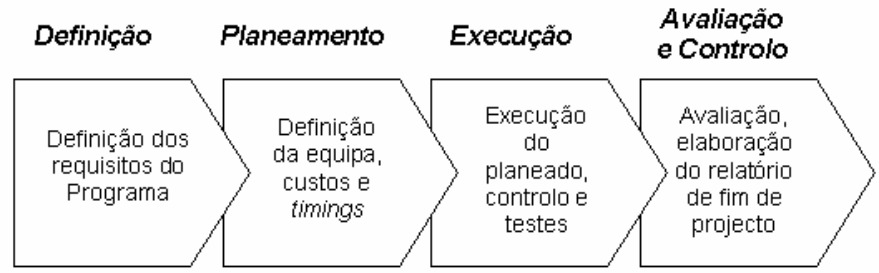


Fig. VII-4: Fases do Programa

Definição do programa – Nesta fase inicial, as necessidades são identificadas de forma estruturada, e definidos os requisitos do programa a desenvolver, bem como os objectivos a satisfazer. Deverão ser igualmente identificados os benefícios esperados com a realização do programa, de modo a permitir a sua "venda" à administração.

Planeamento – Nesta fase é efectuado o planeamento de todas as tarefas do programa, sendo definida a equipa responsável pela respectiva implementação e a quem será apresentado o programa nas suas diversas vertentes: objectivos, tarefas e papéis a desempenhar. É também nesta fase que se planeiam os testes, a formação dos utilizadores e os diversos momentos de informação a toda a Empresa.

Execução – Durante a fase de execução são desenvolvidas as tarefas definidas no planeamento, sendo efectuado o seu controlo e, sempre que necessário, implementadas medidas correctivas. É também nesta fase que se efectuam os testes e a formação dos utilizadores finais.

Avaliação e Controlo – No final do programa, ou de cada projecto que o compõe, são efectuadas a avaliação detalhada da equipa e a

avaliação do programa pela equipa. Após a realização destas apreciações deverá ser elaborado o relatório final que, para além da análise dos desvios (de custos, objectivos e prazos), deverá apresentar as *best practices* desenvolvidas e as propostas de melhorias/necessidades identificadas, que poderão dar origem a novos programas ou projectos.

Recolha de Informação

A informação é a peça fundamental para o controlo de gestão e deverá ser trabalhada desde o momento da aprovação do programa. Deste modo, os fluxos de comunicação formais deverão ser definidos na fase de planeamento do programa, devendo ser equacionadas, desde logo, as necessidades específicas dos seus diversos intervenientes. O fluxo de comunicação definido deverá estar integrado no modelo de gestão estabelecido para o programa (ver exemplo da Fig. VII-5), de modo a assegurar a correcta distribuição de informação formal.

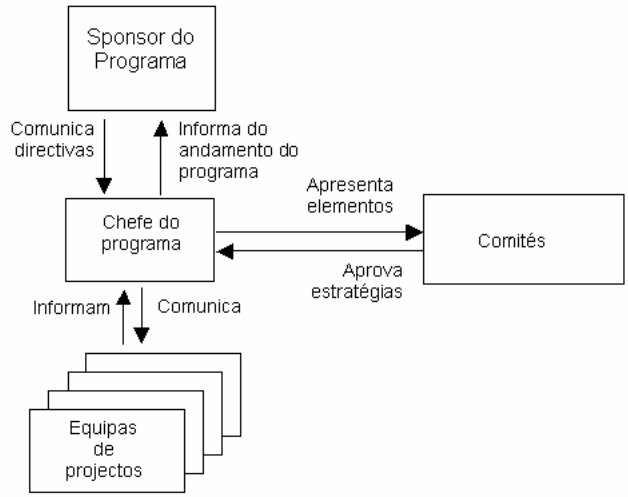


Fig. VII-5: Fluxo de comunicação - Exemplo

Deverá ser igualmente determinado não só o tipo de informação a distribuir, mas também os seus destinatários e respectiva calendarização. Para facilitar esta tarefa, poder-se-á também incluir nos documentos de planeamento um quadro (e/ou diagrama) com os diversos intervenientes do fluxo de comunicação (ver Fig. VII-6).

Lista de Distribuição

Nome	E-mail (ou outro contacto)
Daniela Silva	daniela.silva@endereço.de.mail
Raquel Martins	raquel.martins@endereço.de.mail
Carolina Antunes	carolina.antunes@endereço.de.mail

Fig. VII-6: Lista de Distribuição - Exemplo

No Programa de Segurança a preocupação com a recolha de informação deverá estar sempre presente, não só para obter dados que possibilitem a prevenção de lacunas na segurança ou de indisponibilidades nos sistemas, como também elementos que permitam avaliar se a implementação dos procedimentos definidos foi a correcta.

Dado tratar-se de um programa transversal, o primeiro interlocutor será a própria Administração da Empresa. A informação, neste caso, será predominantemente formal e deverá ser recolhida através de actas das diversas reuniões efectuadas. De forma a optimizar as reuniões, o chefe do Programa de Segurança deverá apresentar antecipadamente uma agenda e os diversos documentos que irão ser discutidos. No final deverá elaborar uma acta que, não sendo contestada, servirá como base de trabalho futuro.

Independentemente do modo como é recolhida a informação, o objectivo da Empresa é obter “informação para informar”: elementos sobre as diversas situações que podem requerer medidas correcti-

vas, com o intuito de adaptação da organização ao meio envolvente.

Assim a recolha não se deve restringir à informação formal. A informação informal é muitas vezes mais rica e permite ter uma atitude pró-activa em relação aos potenciais problemas. É muitas vezes através de "conversas de corredor" que o chefe de programa se irá aperceber de diversas situações críticas sobre as quais deverá agir de forma a neutralizar potenciais problemas.

Exemplo: o chefe do Programa de Segurança deve aproveitar as conversas informais tidas com os administradores de sistemas e outros técnicos para se aperceber se as normas de segurança estão a ser interpretadas adequadamente, ou seja, se as medidas de segurança decorrentes desses documentos estão a ser implementadas.

Não devemos esquecer que a segurança é uma área crítica da Empresa e que deverão ser tomadas medidas logo no momento em que se detecta algum problema. Assim sendo, deverá providenciar-se um esquema de disseminação de alertas, assente em sistemas tecnológicos ou não, tanto para incidentes (por exemplo, um sistema responsável pelo envio de uma mensagem quando um servidor pára), como para vulnerabilidades (pode ser simplesmente o reenvio selectivo de *newsletters* de vulnerabilidades). Desta forma será assegurado o fluir de informação no momento em que surge um problema ou em que a situação se torne crítica. O objectivo destes mecanismos de comunicação será conferir visibilidade aos problemas existentes e permitir a tomada de medidas adequadas.

Outro objectivo da definição de um fluxo de informação para o Programa de Segurança é assegurar que todos os colaboradores sabem a quem recorrer quando há um problema, ou seja, mesmo que não saibam o que fazer, saberão quem devem contactar para obter instruções. Este último ponto é fundamental, dado que pode representar a diferença entre um pequeno incidente e uma crise.

Exemplo: em caso de indisponibilidade do serviço de correio electrónico – a principal forma de comunicação da maioria das empresas –, deverá existir um esquema de aviso para toda a organização (por exemplo, por fax), informando os utilizadores da situação existente e da expectativa de resolução, bem como indicando uma forma de acesso a informação actualizada por parte dos afectados.

O fluxo de informação formal deverá ser estruturado em três fases distintas:

- início do programa;
- implementação do programa; e
- conclusão do programa.

Numa fase inicial deve-se contemplar a informação necessária à definição de requisitos (o que deve ser implementado pelo programa), tentando garantir que a recolha seja o mais abrangente possível, isto é, que todas as áreas relacionadas com o programa são ouvidas, tentando evitar perdas de tempo em discussões improdutivas. Nesse sentido, deverão ser definidos fluxos de informação para as áreas envolvidas no programa, ou que venham a beneficiar directamente com a sua implementação, bem como para a administração.

Após a definição dos requisitos e das características do programa, deverá ser elaborada uma descrição pormenorizada, que será assinada pelas diversas áreas e pela equipa do programa, servindo de garante para o cumprimento do estipulado.

Ao longo de todo o programa, é essencial garantir o correcto funcionamento do fluxo de informação, como forma de atingir os objectivos propostos. Esta troca de dados irá permitir identificar atrasos, indefinições de requisitos, impasses e outros problemas. Ao fazer fluir a informação estarão criadas condições para actuar atempadamente, minimizando o potencial impacto dos problemas.

Um dos modelos de comunicação de carácter genérico, que deverá possuir cerca de quatro ou cinco páginas, servirá para fornecer ao *Sponsor* do programa uma visão sobre o seu andamento, indicando os próximos passos e respectivos riscos, que poderão ser, por exemplo, de escassez de recursos, de indefinição de requisitos, potenciais atrasos em programas relacionados, ou até receio de incumprimento dos prazos estabelecidos. Este relatório deverá ser elaborado pelo chefe de programa, que o entregará ao *Sponsor*, em comité próprio em sede do Conselho Executivo ou Administrativo, ou em reuniões mensais de acompanhamento do programa.

Para elaborar este documento, o seu responsável deverá socorrer-se dos relatórios parciais elaborados pelos chefes de projecto, num modelo próprio, devendo estes, de forma mais detalhada, efectuar uma análise do andamento do programa, identificando as suas principais preocupações e sucessos.

No final do programa deverão ser consideradas diversas fontes de informação, de igual importância, com o objectivo de recolher dados abrangentes que permitam a elaboração adequada do relatório final de programa.

Uma vez que tanto os objectivos de um projecto como os seus beneficiários directos deverão ser conhecidos à priori, deverá considerar-se que o projecto só se encontra oficialmente encerrado após a realização de inquéritos aos utilizadores, ou seja, após recolha de informação sobre o impacto da implementação e da opinião de todos os seus beneficiários.

Exemplo: ao definir uma política de *backups*, os beneficiários (aqueles que produzem a informação que passou a estar protegida) não sentem diferença, a menos que necessitem desse *backup* e ele não exista. Neste caso, poderão considerar-se os responsáveis pela implementação dos *backups* como os beneficiários a auscultar, uma vez que passaram a dispor de um meio para responder às solicitações de reposição de dados perdidos.

O relatório final de programa deverá, como afirmado, ser elaborado pelo chefe de programa, identificando os *milestones* (momentos chave) atingidos, os desvios encontrados, a justificação para os desvios, as *best practices* desenvolvidas ao longo do programa, os problemas ou preocupações da equipa (que poderão originar novos programas), para além de tecer considerações finais. Este relatório deverá ser elaborado em colaboração com todos os elementos da equipa, que deverão dar o seu *feedback* em reuniões de encerramento do programa, de modo a permitir a compilação de toda a informação relevante pelo responsável.

Planeamento

As organizações são entidades em constante mutação pois têm de se adaptar às diversas alterações do meio envolvente. Assim, surgem constantemente desafios, projectos ou programas, mais simples ou mais complexos, mas sempre com uma necessidade comum: a necessidade de planeamento, de definição de objectivos e de afectação de recursos. Esta é uma fase crítica no ciclo de vida de qualquer programa, pois um bom planeamento constitui a base sobre a qual se irão desenvolver as actividades posteriores.

Num programa transversal a toda a Empresa, como é o caso do Programa de Segurança, o planeamento é fundamental para conseguirmos, no final, avaliar a eficácia das medidas tomadas.

Calendário/Actividades

O planeamento de qualquer programa requer detalhe, cujo nível deve ser ponderado, dado que esta actividade demora tempo e consome recursos, sendo, no entanto, essencial a um bom programa. Ao definir os objectivos a atingir, ter-se-ão, pois, de identifi-

car as diversas tarefas a realizar, determinar a altura da sua execução e estimar o número de dias/homem[24] que estas irão consumir.

A calendarização das tarefas de alto nível (ver Fig. VII-7) constitui a base de trabalho para a afectação dos recursos e para a definição das *milestones* do programa.

Calendário do Programa

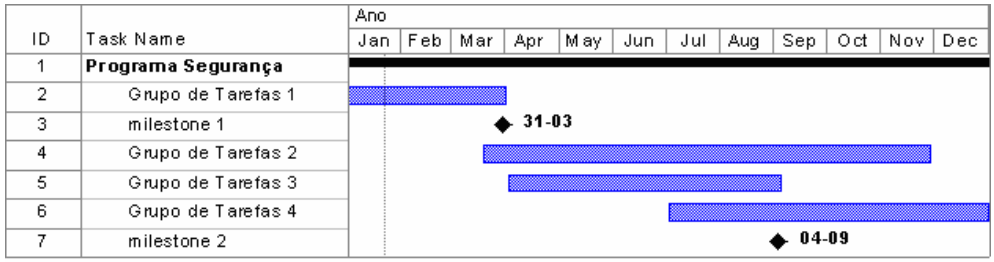


Fig. VII-7: *Gantt* de alto nível (Microsoft Project)

Na fase de planeamento deverá também ser definido o modelo de gestão, composto essencialmente pela identificação dos seus diversos intervenientes, do modo como se relacionam, da sua hierarquia, das suas funções e da calendarização dos momentos de avaliação do andamento do programa.

Num programa com a transversalidade e abrangência do Programa de Segurança, o modelo de gestão é uma peça fundamental, sendo recomendada a definição de um *Sponsor* (patrocinador) ao mais alto nível da Empresa, que deverá assegurar o correcto andamento do programa, impondo a sua força sempre que surjam obstáculos. Deverá também ser definida a metodologia de *reporting* e respecti-

[24] Número de dias completos de trabalho multiplicado pelo número de recursos alocados (por exemplo, dois dias completos x dois recursos = quatro dias/homem).

vos prazos, isto é, quando e como é que o chefe de programa deve reportar ao *Sponsor* o andamento do mesmo, os riscos identificados e os próximos passos. Seguidamente procede-se à nomeação do chefe de programa, que deverá ser sempre que possível o responsável pela segurança na Empresa e a definição da metodologia de *reporting*.

Após esta definição, o chefe de programa estará preparado para passar a uma fase de maior detalhe. No caso do Programa de Segurança, esse detalhe corresponde à determinação das principais actividades decorrentes da análise de risco anteriormente efectuada. Não deveremos contudo esquecer que o Programa de Segurança é uma actividade da Empresa e, como tal, deverá ser comunicado à Empresa, por forma a sensibilizá-la, tanto no seu início como nos diversos *milestones* e sempre que se justificar. Estes momentos deverão também ser calendarizados por parte do chefe do programa.

Afectação de Recursos

A afectação de recursos a um programa nunca é tarefa fácil, pois se por um lado é necessário identificar os elementos que melhor se adaptam às necessidades do programa, por outro temos de considerar a sua possível indisponibilidade.

Num programa com a abrangência do Programa de Segurança Empresarial, será necessário ter em conta as necessidades de afectação de recursos nas diversas áreas, independentemente da sua dependência hierárquica. Contudo, nestes casos, será necessário considerar a "libertação" desse pessoal nos momentos em que devem ser afectados ao programa, pois frequentemente, após a concordância inicial, os recursos não se encontram disponíveis na altura em que as tarefas são realizadas, implicando inevitavelmente deslizes no planeamento. Para garantir que os elementos afectos ao programa o estão na realidade, o chefe de programa deverá negociar primeiro com os superiores hierárquicos dos recursos a

afectar, identificando claramente qual irá ser a sua participação ao longo do programa e o objectivo dessa participação.

Devido às características do Programa de Segurança, este deverá ter afectados recursos das diversas áreas da Empresa, quer do campo das tecnologias de informação, quer das restantes áreas não tecnológicas.

Exemplo: poderemos entender um pouco melhor esta problemática da afectação de recursos considerando a definição dos procedimentos necessários para garantir a continuidade em caso de desastre, que devem ser definidos pelos elementos que executam habitualmente os processos de negócio críticos. Assim, o chefe de programa deverá reunir com as diversas hierarquias, solicitando por um lado a sua colaboração para o projecto (o que servirá também como uma forma de sensibilização para a problemática da segurança) e a ajuda na definição dos recursos mais indicados. Deverá também, apresentar claramente qual a afectação necessária e quais os momentos críticos, de modo a evitar a necessidade de reafectações posteriores.

Só com a clara identificação das necessidades de recursos, com o acordo explícito das suas hierarquias e com a correcta motivação para a participação no programa, é que se disporá de uma base sólida para o arranque. Assim, só a correcta definição da equipa e a afectação adequada e cautelosa dos diversos elementos humanos permitirá garantir o sucesso do programa, uma vez que serão aqueles o motor da sua concretização.

Matriz de Responsabilidades

A matriz de responsabilidades é uma peça fundamental na definição dos papéis dos vários intervenientes no programa, permitindo estipular os diversos passos/actividades e os responsáveis pela decisão, consulta, implementação, etc. (ver Fig. VII-8).

A clara definição dos diversos papéis permite informar todos os participantes no programa das suas responsabilidades, da sua forma de articulação e, acima de tudo, identificar os elementos a quem se deverá recorrer em caso de necessidade.

Esta matriz é uma ferramenta útil na gestão quotidiana do programa, bem como de outras tarefas que envolvam vários recursos. Ao definir os diversos passos de um processo, associando as tarefas aos responsáveis, a pessoas que possam, de algum modo, colaborar em caso de necessidade e a elementos que, em última análise, detenham poder de decisão, garante-se o fluir do processo.

Matriz de Responsabilidades

Recursos / Acção	A	B	C
Tarefa 1	F	A	D
Tarefa 2		F	E
Tarefa 3	F	A	

Legenda: F – Efectua
E - Acompanha Evolução
A - Apoia caso necessário
D - Decide

Fig. VII-8: Matriz de responsabilidades - Exemplo

O Programa de Segurança só tem a beneficiar com a construção de uma matriz de competências, pois ao tratar-se de um programa abrangente, que envolve recursos de todas ou, pelo menos, de diversas áreas da Empresa, é natural que surjam muitas vezes questões relacionadas com competências (“quem faz o quê?”) e com responsabilidades (“quem é o responsável?”). Estas dúvidas

poderão provocar paragens no processo, implicando certamente atrasos na concretização dos objectivos definidos.

Para evitar estes percalços, deverão ser definidos logo à partida, de forma inequívoca, os diversos papéis para as diversas fases do Programa de Segurança.

Exemplo: voltando ao exemplo anterior, na definição de procedimentos de continuidade do negócio deverão ser identificados os diversos recursos das áreas envolvidas. Estes elementos poderão contar com a consultoria dos chefes dos sub-projectos e, em caso de impasse, com a intervenção do chefe de programa. Assim, é garantido o conhecimento dos respectivos papéis por parte de todos os intervenientes e assegura-se a existência de um elemento, claramente identificado, responsável pela tomada de decisões em caso de impasse.

A construção da matriz deverá ser feita de forma cautelosa pois, se por um lado nela deverão estar identificados os diversos passos do Programa de Segurança, por outro deverá ser exposta aos diversos intervenientes e ter a sua concordância relativamente aos papéis aí definidos.

Após a aprovação da matriz pelo *Sponsor* do programa, esta deverá ser apresentada e publicitada junto de todos os intervenientes no programa.

Análise de Custos/Necessidade de Fundo de Maneio

Ao efectuar o planeamento, os diversos custos relacionados com o programa deverão ser projectados, pois só assim se poderá ter a noção real do valor associado ao benefício esperado do programa. Nesta matéria há que considerar diversos custos: desde recursos afectados directamente ao programa (internos e externos) até aos materiais utilizados, deslocações, etc. Todos estes valores deverão ser calculados na fase de planeamento, de modo a identificar o custo total. Para tal, não deverão ser esquecidos nenhuns encargos

ocultos (por exemplo, o custo das reuniões de acompanhamento do programa), uma vez que o seu cálculo promove a optimização (no caso do exemplo, optimização dessas reuniões).

A correcta definição de encargos é a base para, através de uma análise custo-benefício simples, se perceber se será oportuno avançar ou não com o programa. No entanto, esta definição deverá ser inicialmente de alto nível, sendo aceitável um desvio de cerca de 30%, de modo a assegurar a celeridade da orçamentação inicial. Uma vez ultrapassada esta fase, no momento final da decisão de avançar ou não com o programa, será então necessário voltar a calcular os custos de modo mais detalhado, reduzindo a margem de erro para a ordem dos 5%.

No caso da segurança, a definição do benefício é algo por vezes complicado, pois estamos perante situações que poderão nunca acontecer. Neste contexto, o que se torna relevante é saber se a Empresa está ou não disposta a correr esse risco, o que deve ser conseguido através de uma análise criteriosa (ver capítulo "Gestão do Risco") que permita identificar os eixos de actuação da segurança, definindo prioridades para as diferentes actividades. Neste processo deverá considerar-se que os custos, incorridos ao longo de todo o programa, não serão necessariamente lineares. Daí a obrigação de efectuar uma análise das necessidades de fundo de maneio do programa, de modo a garantir que este não será interrompido por indisponibilidade orçamental.

As necessidades de fundo de maneio representam a disponibilidade orçamental necessária para cada período, associadas aos diversos fluxos de caixa. Comprar ou vender algo, hoje, não representa necessariamente uma entrada ou saída de dinheiro hoje, pelo que os prazos de pagamentos e de recebimentos terão de ser tidos em conta.

Exemplo: suponhamos que no mês de Fevereiro será necessário o apoio de recursos externos no valor de € 25.000, com um pagamento de 30% no momento da contratação e o restante a 30 dias, e que será também neces-

sário adquirir equipamento no valor de € 1.000, com pagamento a 45 dias: as necessidades de fundo de maneio para Fevereiro e Março serão as indicadas na Fig. VII-9.

Fundo de Maneio

Fevereiro	**NFM**
Recursos externos 30% x € 25.000	7.500
Março	
Recursos externos 70% x € 25.000	17.500
Equipamento 100% x € 1.000	1.000

Fig. VII-9: Fundo de Maneio - Exemplo

A análise criteriosa das despesas associadas ao programa serve também de base ao estabelecimento de acordos de nível de serviço. Consegue-se, desta forma, a definição do nível de serviço associado à classificação da criticidade do componente (sistema, aplicação, etc.), relacionando o tempo de indisponibilidade (custo de paragem) com o custo da intervenção/prevenção.

Exemplo: um nível de serviço que preveja a reposição do serviço em duas horas requer que o custo de duas horas de indisponibilidade seja superior ao valor necessário para assegurar a reposição do serviço nesse período.

O estabelecimento dos acordos de nível de serviço requer, assim, a avaliação da criticidade da informação (ver “Segurança da Informação” no capítulo “Áreas da Segurança Empresarial”) e a correcta análise dos custos, que vão desde os relacionados com material, aos dos recursos internos, integrando o factor escassez que decorre da disponibilidade limitada dos recursos.

Preços de Transferência

A tendência actual na gestão das organizações passa pelo controlo efectivo dos custos/benefícios dos diversos departamentos, assente em preços de transferência entre os mesmos. Esta análise dos diversos custos e da sua relação causal visa a correcta transferência dos encargos entre os diversos departamentos associados aos serviços prestados, afectando a sua avaliação de desempenho.

Esta metodologia traduz-se em diversos benefícios para a Empresa, pois, para além de permitir a correcta avaliação da capacidade de execução dos seus departamentos, promove uma utilização inter-departamental optimizada dos recursos, particularmente no que respeita aos departamentos de suporte, como é o caso do departamento de Sistemas de Informação. O grande inconveniente desta metodologia prende-se com os encargos associados à montagem e manutenção do sistema de suporte à transferência de custos.

Entre as diversas metodologias utilizadas encontram-se:

- a transferência dos custos dos departamentos de suporte (por exemplo, SI, Contabilidade, etc.) para os departamentos principais (por exemplo, comerciais) com base em percentagens predefinidas;
- a transferência total dos custos na proporção da sua utilização pelos diversos departamentos; ou
- a óptica de micro-empresas, em que são estipulados preços de venda dos serviços (superiores ao custo real) entre departamentos.

A escolha da metodologia a adoptar irá, naturalmente, depender do modelo organizativo, dos custos/benefícios da montagem do sistema de suporte e dos seus valores de manutenção.

No Programa de Segurança poderá ser utilizada uma destas metodologias, uma vez que, devido à sua abrangência, a segurança não deverá ser encarada como um custo exclusivo de um único departamento (tradicionalmente o de Sistemas de Informação), uma vez

que beneficia a Empresa como um todo. Assim, o programa poderá adoptar uma lógica de preços de transferência, permitindo a deslocação dos custos para os seus reais beneficiários.

Exemplo: considerando a implementação de ferramentas de segurança lógica nos portáteis da Empresa, o custo da sua implementação poderá ser repartido pelos departamentos beneficiados, de acordo com a percentagem do número total de portáteis afectos a cada um.

Qualidade

Outro factor relevante na fase de planeamento é a preocupação com a qualidade. No Programa de Segurança serão alterados sistemas e processos, sendo necessário garantir que estes irão funcionar correctamente, com o menor impacto possível sobre o trabalho quotidiano dos colaboradores. Desta forma, o planeamento deverá incluir diversas fases que permitam garantir a qualidade satisfatória dos resultados, para além do produto desenvolvido, do processo redefinido e das tarefas efectuadas.

A garantia da qualidade deverá ser conseguida através da definição da melhor metodologia para atingir os objectivos propostos e para garantir que o resultado do programa é adequado aos requisitos predefinidos.

Actualmente, considera-se que a qualidade é a grande preocupação das organizações, que procuram uma postura de Qualidade Total. Porém, olhando para o dia-a-dia das nossas empresas, verificamos que a qualidade é por vezes esquecida em procedimentos básicos, mas essenciais. Para que tal não aconteça, deve-se começar por tentar incutir a necessidade da qualidade e torná-la um dos objectivos principais de todos os intervenientes na organização. Só depois se poderá pensar em Qualidade Total.

Na fase de planeamento deverão definir-se as diversas tarefas, a ordem pela qual são realizadas, os fluxos e o relacionamento entre elas. Logo, é a partir desta fase que a qualidade deve constituir uma

preocupação, procurando a melhor metodologia e a melhor forma de implementar o programa.

A definição do modelo de gestão e a necessidade de acompanhamento do programa por parte do *Sponsor* é uma primeira contribuição para a qualidade, pois o olhar crítico de alguém "externo" irá certamente analisar, sem qualquer tipo de influência, os métodos e procedimentos escolhidos.

Ao longo de todo o Programa de Segurança deverão ser efectuados diversos tipos de testes, com objectivos diversos, consoante a fase em que o programa se encontre. Inicialmente serão necessários testes para verificar a conformidade do planeamento com os requisitos definidos e com os objectivos (de negócio ou não) associados a esses requisitos, enquanto que, durante a implementação, serão necessários testes adicionais, de validação/aceitação dos resultados.

Contudo, caso se pretenda um projecto de qualidade, estas análises não se deverão esgotar aqui, pelo que se deverão efectuar também testes de impacto do projecto, isto é, identificar as alterações provocadas aos procedimentos e métodos de trabalho.

A realização deste tipo de testes permite identificar a melhor metodologia para a implementação, assegurando a qualidade dos produtos finais e a sua adequação às reais necessidades dos beneficiários, e garantindo que a sua realização não irá, por exemplo, atrasar a produção, o que poderá traduzir-se num atraso para o cliente.

É necessário pensar na qualidade de forma abrangente logo desde o início, pois quanto mais tarde se detecta um erro, mais complexa, difícil e onerosa é a sua resolução, dificuldade essa que, em algumas áreas (por exemplo, no desenvolvimento de software) chega a ser exponencial.

Implementação

Implementar um programa não é tarefa fácil. Acarreta muita dedicação e compromisso, implicando um pulso de ferro e adaptabilidade. Acima de tudo é necessária capacidade de liderança e de motivação da equipa, fazendo as coisas acontecer como planeado e, por vezes, superando mesmo o planeado. Como se liderar uma equipa não fosse já uma tarefa suficientemente difícil e consumidora de tempo, será ainda necessário planear a implementação mais eficaz do programa no terreno. Para além disso, há que contar com a gestão das mudanças, o que representa muitas vezes um esforço mais complexo que a actividade principal, e com riscos mais críticos.

Gestão da Equipa

A gestão da equipa do programa, dadas as suas particularidades, difere em alguns aspectos da gestão de uma equipa de trabalho comum. Este é um grupo com objectivos bem definidos e delimitados no tempo, muitas vezes agregando pessoas de diferentes áreas e que, temporariamente, deverá reportar a um responsável que se poderá encontrar fora da sua hierarquia definida. A equipa do programa deverá iniciar os seus trabalhos logo após a negociação dos recursos com o respectivo superior hierárquico. Para tal, deve ser realizada uma reunião de lançamento do programa, em que serão apresentados os objectivos globais e individuais, o papel de cada interveniente e os prazos disponíveis. Esta reunião deverá servir para apresentar o programa à equipa e, também, para lhes “vender a ideia”, sendo este o início do arranque de um processo de motivação que só deverá terminar na conclusão do projecto.

Um dos factores de sucesso é, precisamente, a motivação das equipas, não só pela dedicação aos objectivos, pela sua disponibilização para reportar a um novo “chefe”, mas também por serem um factor decisivo no processo de mudança que todos os programas

acarretam. Desta forma, a motivação e envolvimento da equipa terá uma importância extraordinária.

Um programa traduz-se, inevitavelmente, numa mudança que deve ser cautelosamente introduzida na Empresa. Assim, desde o momento em que surge o sentido de urgência da necessidade de mudança, esta deverá ser difundida pela organização, transmitindo uma visão clara de onde se pretende chegar com determinado programa. Esta visão deverá então ser traduzida em estratégias, ou seja, em diversas componentes do Programa de Segurança.

Uma vez definidos os objectivos e a forma de os atingir, a equipa irá constituir o veículo privilegiado de transmissão de informação sobre a mudança, não se podendo esquecer que será esta informação, veiculada durante o programa, que muitas vezes cria uma predisposição positiva ou negativa para a mudança.

Gestão da Mudança

Para que a mudança associada à implementação do programa se materialize facilmente, há que garantir que a necessidade de mudança é sentida na organização. A verificação da incorrecção ou da insustentabilidade da situação actual é meio caminho andado para conquistar adeptos da mudança. Caso esta não seja sentida por todos, as modificações serão mais difíceis, sendo frequente, nesta situação, ouvir frases como “para quê mudar, este sistema funciona tão bem”.

Sempre que seja este o caso, o chefe do programa deverá apoiar-se, por exemplo, em acções de sensibilização onde sejam divulgadas as diversas vulnerabilidades existentes, como forma de demonstrar essa necessidade. Para além dela, há que assegurar que a visão é partilhada, isto é, que todos sabemos onde queremos chegar e, preferencialmente, que todos sabemos o que irá ser feito para lá chegar. Possuir uma visão e estratégias comuns é um dos factores críticos da mudança, o que deverá ser garantido pelo chefe

de programa, tendo especial atenção para com as áreas da Empresa que serão afectadas.

Como foi referido anteriormente, outro factor chave da mudança é a comunicação. Assim, é de extrema importância dar a conhecer o programa, pois se este for partilhado, se motivar interesses e adeptos, constituirá certamente um factor facilitador da evolução, uma vez que, ao ser conhecido, suscitará curiosidade e levará os diversos elementos da Empresa a envolverem-se, questionando a situação actual e considerando a sua modificação.

Nada se consegue sem a motivação adequada. Para tal, ao efectuar o planeamento do programa, o seu responsável deve tentar garantir pequenas vitórias a curto prazo, isto é, identificar claramente *milestones* (momentos chave) que, ao serem atingidas, possam ser celebradas. Estas pequenas celebrações motivam para a mudança, estimulando a continuidade do processo e incentivando a equipa a trabalhar nesse sentido.

Outro elemento a considerar, em termos de alterações ao *status quo*, é o seu impacto sobre o modo como os diversos colaboradores realizam as suas funções e efectuam determinado procedimento. Estas alterações, maiores ou menores, terão impacto no dia-a-dia dos colaboradores, pelo que a definição do plano de formação deve ser efectuada com algum cuidado. Garantir uma formação e acompanhamento correctos são essenciais para derrubar algumas barreiras de resistência à mudança, pois mudar é sempre um salto para o desconhecido e é sempre bastante mais difícil. Para facilitar a implementação deverão também identificar-se alguns elementos chave (preferencialmente colaboradores da mesma área organizacional dos formandos), que terão formação intensiva devido à sua maior motivação/apetência para a novidade com vista a incentivar posteriormente com a sua capacidade de comunicação. Chegada a fase de implementação, estes elementos estarão assim acessíveis e disponíveis, servindo como pontos de acompanhamento e estabilidade e constituindo-se como um primeiro nível de *helpdesk* muito informal.

Estas são algumas das questões que devem ser consideradas, de modo a garantir uma mudança mais suave e com maior percentagem de sucesso. Não sendo únicas, nem sendo certamente a "receita mágica", devem, contudo, ser tidas em conta, uma vez que comunicar, ter todos os membros da equipa focados nos objectivos e possuir elementos facilitadores da mudança, foram certamente factores críticos para o sucesso de muitas das mudanças já implementadas nas organizações.

Como Envolver o Negócio na Segurança

O Programa de Segurança é um programa para o negócio, na medida em que a necessidade de garantir a segurança e disponibilidade da informação é, acima de tudo, uma necessidade do negócio. Assim, este deverá ser envolvido desde o início do programa, quer seja na definição do Plano de Continuidade do Negócio ou, simplesmente, quando se trata de classificar a criticidade da informação a proteger e os respectivos níveis de serviço. Contudo, a participação do negócio não deve ficar por aqui. Toda a Empresa deverá ser envolvida na segurança, sendo necessário para tal que o chefe de programa efectue diversas acções de sensibilização, cativando o empenho de todos os colaboradores da Empresa com vista à melhoria da sua segurança.

A participação do negócio no Programa de Segurança pode ocorrer a diversos níveis, designadamente:

1. na identificação dos processos de negócio;
2. na identificação dos proprietários da informação;
3. na classificação da informação;
4. no estabelecimento de acordos de nível de serviço (SLA) ; e
5. na sensibilização e na realização de questionários.

A identificação dos processos de negócio e classificação da sua criticidade requer, naturalmente, o envolvimento da Empresa como um todo, uma vez que só as diversas áreas do negócio possuem as competências necessárias à definição e identificação dos seus processos, destacando os mais críticos. Nesta acção é essencial garantir a participação de elementos das diversas áreas não TI da Empresa, pois só assim se garantirá a existência de um conhecimento profundo desses processos críticos.

A identificação dos proprietários da informação é uma questão crucial para o desenvolvimento da segurança, sendo necessário, para tal, identificar o responsável por essa informação, a quem deverão ser reportados os problemas e atribuída a autoridade para facultar acessos. Assim, há que definir relacionamentos e regras, identificando os fluxos de comunicação entre os sistemas de informação e os proprietários da informação armazenada e processada por esses sistemas, bem como sensibilizar esses mesmos proprietários para os seus próprios requisitos de segurança.

A classificação da informação é o processo que irá permitir a protecção diferenciada dos diversos suportes de dados, permitindo uma eficiente gestão dos recursos necessários para a protecção dos bens da Empresa. Esta actividade deverá ser efectuada tendo em conta que a criticidade da informação pode decorrer tanto das necessidades próprias do negócio, como de questões legais.

Exemplo: uma base de dados com informação pessoal de clientes é necessariamente informação crítica, em termos de confidencialidade e de integridade, com requisitos muito específicos de protecção (ver “Padrões e Legislação”).

O ponto de partida deste processo deverá ser a apresentação aos diversos proprietários dos dados das definições dos diferentes níveis de classificação, se possível com métricas, demonstrando a necessidade de segmentação da informação com vista à sua protecção eficiente.

A classificação do nível de criticidade da informação só será útil se tiver como consequência um tratamento diferenciado. Isto é, será inútil classificar o requisito, por exemplo, de disponibilidade da informação crítica se depois, em situações de indisponibilidade, isso não se reflectir em processos de recuperação prioritária dessa informação.

De modo a garantir que os diferentes elementos são tratados de acordo com a sua criticidade, devem ser definidos acordos de nível de serviço (SLA), elaborados necessariamente em estreita colaboração com os proprietários da informação. Nestes acordos devem ser identificados os procedimentos a cumprir, relacionados com a garantia dos requisitos de protecção da informação em causa, sendo definidas métricas para o cumprimento dos mesmos (por exemplo, o tempo necessário à resolução de indisponibilidades).

Garantir a segurança do conhecimento detido pela Empresa não passa apenas pelos SLA ou pela definição de regras, mas também pela sensibilização em matéria de segurança. Tal pode ser conseguido a diversos níveis, devendo ser sempre encarada como uma prioridade, uma vez que parte significativa dos ataques registados nas Empresas vêm do seu interior.

A sensibilização poderá ser efectuada em sessões realizadas pela equipa de segurança, que de uma forma ligeira transmitirá as diversas preocupações de segurança, apresentando exemplos reais de perigos, como é o caso da engenharia social. Outro meio de sensibilização acessível ao Programa de Segurança são os mecanismos de comunicação formal da Empresa (*newsletters*, *e-mail*, *Intranet*, etc.), através dos quais se podem apresentar as regras de segurança mais simples (por exemplo, regras alusivas à constituição e alteração periódica das palavras-passe), não esquecendo sempre de dar a conhecer as razões por trás da existência de tais orientações e os seus principais objectivos.

No final do programa, e nos seus momentos chave, deverá ser sempre avaliada a eficácia e receptividade das medidas implemen-

tadas até à data, analisando o sucesso verificado na adopção das mudanças.

No Programa de Segurança, o envolvimento é uma questão essencial, pois a segurança da Empresa começa nos seus colaboradores. Assim sendo, o impacto das medidas introduzidas deverá ser avaliado, analisando a sua receptividade e adequação aos processos de trabalho afectados, uma vez que só assim será possível retirar conclusões quanto ao cumprimento dos objectivos delineados. Desta forma, deverão ser elaborados questionários que permitam ao chefe de programa percepcionar o resultado das implementações que efectuou para que possa, caso necessário, promover as medidas que permitam melhorar esses resultados, tais como sessões de formação, ajustes a procedimentos, etc.

Ao dificultar, ou até impedir, o *feedback* por parte dos visados pelo programa, estará a criar-se uma parede de resistência, a princípio imperceptível, que irá crescendo, podendo ser já intransponível quando finalmente se tornar visível. A abertura do canal de comunicação conseguida pela realização de inquéritos é essencial, não só para avaliar as mudanças e o seu impacto, mas também para aferir da realização de mais-valias concretas.

Timing para Adopção de Tecnologias

A adopção de tecnologias pelas empresas varia consoante as suas características e objectivos. Em termos de comportamento, uma organização poderá posicionar-se tanto como “inovadora”, adoptando a tecnologia assim que esta surge, com todos os riscos e benefícios a ela inerentes, ou poderá ser “conservadora”, adoptando a tecnologia apenas quando esta se encontra já consolidada e aceitando o risco de “perder o comboio” e ficar para trás face à concorrência.

Apesar de não existirem “receitas” para a adopção das tecnologias, pois cada caso é um caso, deverá tentar efectuar-se uma análise detalhada, considerando as várias alternativas, os benefícios e os

riscos de cada postura. Relativamente ao Programa de Segurança, esta análise ganha ainda maior relevância uma vez que uma falha na tecnologia poderá ser mais grave do que a sua inexistência.

O interesse despertado pelas diversas tecnologias segue uma evolução característica e conhecida, apresentada na Fig. VII-10. Existe uma fase inicial de crescimento acentuado, associada ao aparecimento da nova tecnologia, repleta de esperanças mas imatura, dando início a uma fase ascendente na sua popularidade, que não é, no entanto, acompanhada por um amadurecimento significativo. A partir do momento em que o mercado separa "o trigo do joio", há um ajuste da realidade, através de uma desinflação das expectativas. Finalmente, a tecnologia entra num processo de amadurecimento sustentado que a caracterizará até ao fim da sua vida.

Do ponto de vista do investimento tecnológico, e na perspectiva da segurança, a adopção de tecnologias nas duas primeiras fases acarreta necessariamente diversos riscos, tais como o desaparecimento do produto ou do fabricante, a presença de uma quantidade inusitada de vulnerabilidades por remover, o aparecimento posterior de novos *standards* incompatíveis com a tecnologia adoptada, etc. Na óptica da segurança, a maturidade é certamente preferível, embora a rápida evolução do ambiente tecnológico requeira a introdução de novos controlos, implicando necessariamente a adopção de novas tecnologias.

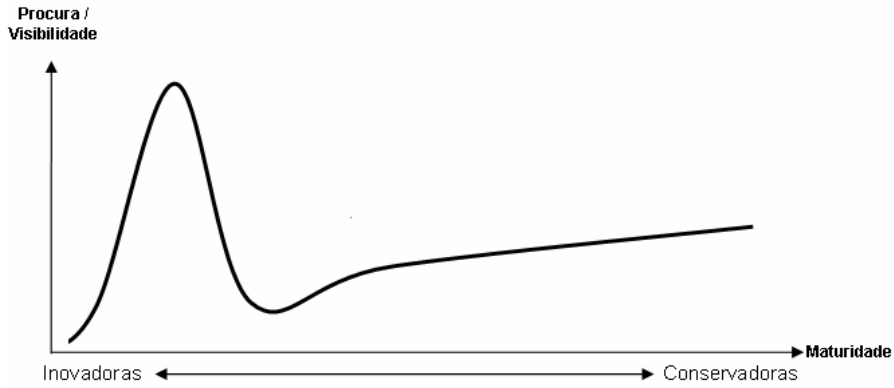


Fig. VII-10: Adopção de tecnologias

Do ponto de vista funcional, os diversos pontos de adopção possíveis de novas tecnologias, ao longo do seu ciclo de vida, representam vantagens e riscos. A introdução de uma tecnologia muito recente permite, regra geral, colher os louros da inovação, correndo-se contudo o risco da tecnologia se revelar apenas uma promessa ou até de apostar num fabricante que não sobreviva a médio prazo. Por outro lado, ficar para trás e adoptar a tecnologia somente quando esta se encontrar consolidada, traz-nos a segurança da sua estabilidade e continuidade, devido à adopção de um *standard* de facto, mas à custa das vantagens auferidas pelos nossos competidores que tenham adoptado essa tecnologia logo no seu início.

Uma vez que funcionalidade e segurança terão de ser equacionadas no processo de selecção das tecnologias a adoptar pela Empresa, será necessário efectuar uma análise do risco e dos benefícios esperados, evitando a todo o custo a tentação da "tecnologia pela tecnologia", garantindo a tomada de decisão verdadeiramente adequada à Empresa.

Controlo/Avaliação

Controlar o andamento do programa e os seus resultados, avaliando o seu impacto e os seus custos, deverá ser uma preocupação que começa logo na fase de planeamento.

Para o correcto acompanhamento do programa será necessário definir a metodologia de controlo e avaliação, de modo a que se consigam comparar os resultados com os objectivos definidos inicialmente, analisando e quantificando os desvios e identificando as suas causas, de modo a retirar conclusões para melhorar programas futuros. Uma vez que a Empresa é uma entidade em constante mutação e aprendizagem, o controlo e avaliação dos seus programas deverá ser um dos motores dessa evolução, aprendendo-se com os erros cometidos e divulgando e reutilizando as *best practices* identificadas.

O controlo e avaliação do Programa de Segurança é um elemento essencial, uma vez que o impacto de potenciais erros ou do incumprimento dos objectivos predefinidos poderá ter um custo muito elevado para a Empresa.

Exemplo: a ocorrência de um desastre após o incumprimento do objectivo de criação do plano de recuperação de desastre não será encarado, certamente, com bons olhos em qualquer Empresa.

O controlo do programa deverá ser constante e formal, devendo ser predefinidos os momentos em que o programa será avaliado e os parâmetros dessa avaliação. Contudo, esta definição pode ser revista caso necessário, com a introdução de novos momentos de controlo. Só com um acompanhamento próximo e atento é que serão identificados atempadamente os desvios ocorridos, permitindo uma actuação no sentido de minimizar os danos (efectivos ou potenciais) por eles causados. O preço a pagar por falhas no acompanhamento poderá ser a detecção tardia de desvios, possivelmente tarde demais para permitir a correcção do problema, o que poderá até pôr em causa o próprio programa. Assim, há que estar atento, recolher a informação de forma atempada e agir sempre que necessário. Nesta área, mais uma vez, a função do chefe do programa é essencial, pois este deverá estar alerta e próximo dos acontecimentos, para garantir que a informação recolhida é tanto fidedigna como relevante.

Sendo afectados recursos de todas as áreas da Empresa, que reportam ao chefe de programa e, simultaneamente, ao seu superior hierárquico, a tarefa de controlo torna-se mais complexa, mais exigente e crucial. Uma vez que os recursos estão na base de sustentação do programa, o seu controlo é essencial, sendo aqui também que se registam os maiores desvios. Por outro lado, este é, também, o factor que mais facilmente pode ser ajustado para “salvar” os prazos do programa e é muitas vezes pelo empenho e dedicação dos recursos que se conseguem atingir os objectivos delineados, sendo eles afinal quem faz a maior diferença.

A afectação dos recursos deverá ser controlada e avaliada ao longo do programa, tanto em termos de horas alocadas, como através da verificação da percentagem de objectivos atingidos/tarefas concretizadas.

O controlo dos recursos poderá ser efectuado com diversas periodicidades: relatórios semanais, mensais, etc. Este controlo pode ser realizado com a utilização de ferramentas mais ou menos elaboradas, como o Microsoft Project (que poderá ser disponibilizado em rede aos elementos do programa de modo a que registem a sua afectação e a concretização das diversas tarefas definidas). Na escolha da ferramenta a utilizar por equipas de maior dimensão, as dificuldades encontradas poderão, no entanto, não compensar os benefícios obtidos, sendo então possível optar pela utilização de uma base de dados alternativa, partilhada, para a informação relevante.

Uma vez que o objectivo do controlo é deter informação sobre o número de horas realizadas por determinado recurso no programa e a percentagem de concretização das diversas tarefas, é possível utilizar uma metodologia mais simplista, como a utilização de um modelo de *reporting* composto por folhas de cálculo, por exemplo, do Microsoft Excel, que deverão ser preenchidas e enviadas, com uma periodicidade estipulada, ao chefe de programa. Este, por sua vez, irá compilar a informação recebida dos diversos elementos da sua equipa.

O controlo dos recursos deverá ser efectuado de forma simples mas eficaz, isto é, não se deverão sobrecarregar os recursos com a elaboração de *reporting*s muito bonitos e complexos, desviando-os da sua tarefa principal (completar adequadamente as actividades do programa), mas antes obter com periodicidade regular, dependente da dimensão do programa e das suas diversas fases, a informação necessária para apurar o andamento das actividades e possibilitar a actuação nos momentos críticos.

A garantia de que o programa corre conforme planeado só é possível se forem incluídos diversos testes no planeamento, de modo a

verificar se os controlos introduzidos pelas actividades funcionam realmente e se os objectivos são verdadeiramente atingidos. As metodologias de teste variam, sendo a mais comum a realização de testes no final do programa, embora em algumas áreas, tais como o desenvolvimento de software, também seja comum a realização de testes ao longo do desenvolvimento.

Um factor a considerar, neste planeamento, é que existem estudos que revelam que quanto mais tarde é descoberto um problema, mais cara fica a sua resolução, pelo que os testes deverão ser efectuados o mais cedo possível e persistir ao longo de todo o ciclo de vida do programa. Segundo esta metodologia, estas análises deverão ser efectuadas logo aos resultados da especificação de requisitos, pois é neste momento que se verifica se o que é proposto realizar-se satisfaz plenamente os objectivos, Caso isso não se verifique, devem-se efectuar correcções, caso fossem realizadas mais tarde, implicariam certamente custos de adaptação muito superiores, uma vez que este tipo de erros pode implicar a redefinição da abordagem aos problemas.

Independentemente da metodologia utilizada, é necessário garantir o cumprimento dos objectivos e certificar que os controlos (por exemplo, software desenvolvido, novos procedimentos a implementar, etc.) são consistentes e não representam, na realidade, grandes perturbações que possam trazer prejuízos à Empresa. Para tal, será necessário simular a inserção do controlo com a finalidade de tentar garantir que este poderá ser implementado sem grandes surpresas.

A equipa de testes pode ser externa à Empresa e contratada para o efeito, embora a situação mais comum seja pertencer à equipa do programa, composta em parte pelos utilizadores da área afectada pelo programa. Independentemente da sua origem, esta equipa deverá ter um planeamento detalhado dos testes a realizar, os respectivos prazos, e deve perceber quais os seus objectivos, de modo a actuar como uma primeira frente de controlo, podendo sugerir

melhorias aos testes, ou até mesmo ao desenvolvimento/ implementação do programa.

O controlo da execução e dos resultados dos testes planeados deverá permitir, através do *reporting* ao chefe de programa e ao *Sponsor*, a adopção das medidas necessárias à correcção de desvios às especificações. Assim, será necessário garantir que ao longo do programa o *reporting* definido é cumprido, quer se trate de *reporting* dos elementos da equipa ao chefe de programa, quer deste ao seu *Sponsor*.

A informação deverá circular em dois sentidos: a equipa reporta ao chefe de programa, que por sua vez reporta ao *Sponsor* e, no retorno, existirá um segundo canal, que assegurará o fluir de informação *top/down* e entre os diversos elementos da equipa, de modo a garantir que todos estão sintonizados com os objectivos e com o andamento do programa.

A formação tem um papel fundamental no sucesso da implementação de um programa, pelo que deverá ser definida como mais uma fase no momento de planeamento. Este é mais um ponto fulcral no sucesso dos programas, pois ao ministrar formação, o processo de mudança é facilitado pela apresentação das novas metodologias e ferramentas, garantindo que os diversos colaboradores da Empresa saberão como actuar adequadamente nos momentos chave de implementação. Garantir o conhecimento “do que fazer” e “como o fazer” diminui a ansiedade do desconhecido, que representa um dos factores de insucesso dos programas de mudança.

O controlo da formação deverá identificar se estas actividades se realizaram, quem participou e, acima de tudo, recolher informação junto dos formandos, para aferir se a formação foi eficaz e se os objectivos propostos foram alcançados. Para tal, o chefe de programa, em conjunto com a área que controla as acções de formação, deverá elaborar um inquérito, a distribuir a todos os formandos, que permita aferir a eficácia da acção e a opinião geral dos seus frequentadores. Estes dados deverão ser coligidos e integrados no *reporting* do chefe de programa ao *Sponsor*, que poderá assim

apresentar as suas considerações sobre a formação, a sua eficácia e adequação.

A identificação de uma linha crítica constitui um auxiliar à análise da evolução do programa, em que são destacadas as tarefas cujos desvios terão implicações directas sobre o mesmo. Estes pontos, essenciais ao cumprimento atempado dos objectivos propostos, deverão ser controlados com maior atenção e rigor, pois desvios nestas actividades trarão certamente desvios significativos ao programa. Assim sendo, o chefe de programa deverá prestar especial atenção aos pequenos desvios existentes nestas actividades, de modo a agir quanto antes, de preferência de forma pró-activa, minimizando os atrasos. As causas dos desvios nesta linha deverão ser sempre analisadas detalhadamente, bem como as suas implicações finais.

Para além da análise atenta dos desvios à linha crítica do programa, o seu responsável deverá também analisar as tarefas que terão impacto sobre as actividades da linha crítica e que, embora numa primeira análise não sejam essenciais, possam vir a ser incorporadas nesta linha, caso se registem desvios significativos nas mesmas.

O controlo e avaliação de um programa poderá também ser efectuado através da realização de auditorias, que poderão ser internas e/ou externas, consoante o impacto esperado do programa no negócio. Estas auditorias visam aferir tanto o andamento do programa como a eficácia das medidas tomadas, permitindo controlar, por exemplo, se os procedimentos criados “no papel” estão a funcionar na prática.

Analisando o Programa de Segurança, as suas características intrínsecas e transversalidade, e os impactos relevantes em caso de incidente, facilmente se poderá concluir que se trata de um programa que deverá ser auditado, de modo a determinar atempadamente se os seus objectivos estão a ter o resultado esperado. Esta auditoria deverá incidir tanto sobre os controlos implementados, como sobre as questões técnicas subjacentes à estrutura dos sis-

temas de informação, isto é, a auditoria deverá garantir, não só que os sistemas funcionam no modo previsto, mas também que esse modo é adequado à Empresa. Esta avaliação deve verificar igualmente, por exemplo, a existência de níveis diferenciados de acesso à informação e o cumprimento dos requisitos de segurança estabelecidos por lei.

As questões anteriormente referidas também devem ser colocadas sob a alçada da auditoria interna da Empresa, o que implica a garantia de que a equipa de auditoria conhece os sistemas da Empresa, as regras existentes e os procedimentos definidos.

A auditoria tem duas funções básicas no que respeita a este programa: verificar o seu andamento e o da introdução dos controlos e validar a eficácia final do programa. Uma auditoria anual, por parte de uma entidade externa, irá assegurar a recolha de informação independente sobre a eficácia dos controlos introduzidos e, em última análise, a obtenção de indicações sobre os desvios existentes que possam contribuir para a melhoria da análise de risco.

Ao longo do programa, a auditoria interna poderá actuar como um elo do processo de controlo. Isto é, em caso de necessidade, poder-se-á solicitar à auditoria uma análise do andamento do programa, das suas diversas actividades, dos custos incorridos, etc. Esta avaliação poderá actuar em caso de desvios graves como uma garantia para o chefe de programa e para o *Sponsor* de que os desvios são realmente os já detectados, e também como forma de pressionar os elementos da equipa no sentido de cumprirem o que estava definido. Estas auditorias intermédias poderão ser planeadas logo no início do programa, para os seus momentos chave, ou então serem solicitadas pelo chefe do programa ou pelo *Sponsor*, em caso de necessidade.

No final, deverá ser sempre efectuada uma auditoria que permita avaliar se os documentos de encerramento do programa são fidedignos (por exemplo, se o relatório de custos está correcto) e verificar também a eficácia das medidas entretanto implementadas.

No âmbito da auditoria interna, será necessário garantir a introdução, nos procedimentos regulares de auditoria, da verificação dos controlos de segurança, como modo de garantir que todos os anos se efectua pelo menos uma análise dos procedimentos de segurança da Empresa que detecte os riscos elementares presentes e, caso necessário, despolete os processos de correcção dos controlos.

Exemplo: se o Plano de Continuidade do Negócio da Empresa requer a definição de um procedimento de contingência para cada processo crítico, a auditoria interna deverá verificar, ao analisar os processos, se todos possuem o respectivo procedimento de contingência.

Todas as auditorias efectuadas à área de segurança deverão envolver o responsável pela segurança da Empresa, ou algum elemento chave da sua equipa, utilizando assim o conhecimento profundo detido por estes elementos como mais-valias necessárias a uma avaliação eficaz.

No processo de avaliação final, o chefe do Programa de Segurança deverá avaliar a sua equipa, indicando, inclusivamente, se esta era adequada. Caso seja possível, esta análise deverá recolher ainda as opiniões dos participantes, incluindo os elementos de todas as áreas da Empresa envolvidos no programa.

Ao avaliar a equipa e a execução do programa será possível aprender com o esforço realizado e com os erros cometidos. Um ponto importante da análise final é, então, a identificação das *best practices* encontradas, isto é, metodologias de implementação com bons resultados e que contribuíram para o (sucesso do) projecto. Após a identificação das *best practices*, estas deverão ser divulgadas no seio da Empresa, para que a organização possa evoluir com base nelas. Para que tal aconteça, o chefe do programa deverá efectuar um relatório simples que apresente as *best practices* de forma sucinta, que possa ser facilmente divulgado e assimilado pela Empresa, por exemplo, através da sua *Intranet*, para que todos possam ter acesso a essa informação e saibam a quem recorrer caso

pretendam aprofundar alguma questão. Desta forma, este relatório deverá ser elaborado com o cuidado de não possuir um conteúdo demasiado técnico.

Como anteriormente referido, o finalizar de um programa deverá caracterizar-se não só pela comemoração e pelos elogios habituais à equipa (quando o programa corre bem, naturalmente), mas também por uma fase de avaliação, análise e elaboração de relatórios pelo chefe de programa e pelos seus colaboradores.

O relatório final deve apresentar os principais desvios registados no programa e resumir as suas causas, realçando também os principais feitos do programa, ou seja, as principais actividades realizadas e os resultados práticos para a organização. Esta é uma questão crucial no relatório final, uma vez que serão as medidas implementadas, por vezes pouco visíveis, que trarão maiores benefícios para a Empresa. Para além dos resultados finais, este documento deverá também apresentar os resultados dos questionários efectuados aos formandos e às áreas "afectadas" pelo programa, bem como apresentar propostas de melhoria, propostas essas que poderão incluir a alteração dos procedimentos de gestão de programas.

O relatório de fim de programa é muitas vezes o primeiro passo para a definição do Programa de Segurança do período seguinte, uma vez que, se elaborado de forma cuidada, poderá realçar diversas questões que deverão ser enquadradas na análise de risco que antecederá o planeamento do Programa de Segurança subsequente.

Conclusão

O Programa de Segurança, pela sua abrangência e importância para a Empresa, tem características únicas, que devem ser analisadas com muito cuidado. Ao tratar-se de um programa cujos desvios poderão ser gravosos para a Empresa, deve prestar-se especial atenção para com todos os desvios encontrados, garantindo que se

trata de um processo de aprendizagem para todos os intervenientes, do princípio ao fim.

Para o sucesso deste programa transversal conta também, de forma significativa, a escolha da equipa adequada e a divulgação do programa à Empresa, o que irá permitir um alinhamento de objectivos entre todos os participantes.

O controlo efectivo das diversas actividades ao longo de todo o programa permitirá, por um lado, agir de forma pró-activa na resolução dos problemas e dificuldades que poderão surgir e, por outro, medir a eficácia e eficiência de todas as metodologias implementadas.

Terminologia

Activação (do Plano)	Início da implementação dos procedimentos de recuperação. Este processo é despoletado pela Declaração de Desastre (ver “Declaração”).
Actividade de suporte	Actividades de produção, tecnológicas, que suportam os processos do negócio; o terceiro e último nível da Cadeia de Valor de Porter.
ALE	*Annual Loss Exposur*e: exposição anual à perda.
Ameaça	Indicação de um dano iminente.
Análise de Impacto no Negócio	*Business Impact Analisys* – BIA: Análise efectuada ao nível da gestão por forma a identificar o impacto da perda de recursos.
Best practices	Melhores práticas: processos óptimos para a realização de determinada tarefa
Centro de Recuperação	Instalações alternativas onde são armazenadas cópias de segurança dos dados da empresa e onde poderão ser realizadas as tarefas de recuperação de funções críticas (em caso de desastre).
Confidencialidade	Característica da manutenção do segredo de determinada informação.
Contenção	Actividades de limitação do impacto de um desastre realizadas durante a contingência. Exemplo: evacuação de pessoal durante um incêndio.

Contingência	Período entre o início do incidente e a declaração de desastre pela Administração.
Continuidade (do negócio)	Disciplina de protecção contra desastre que tem como objectivo a manutenção do funcionamento das funções críticas da Empresa.
Controlo (de risco)	Medidas de prevenção contra os riscos que visam a sua evasão, redução, aceitação ou transferência.
Declaração (de desastre)	Reconhecimento formal da existência de um desastre na Companhia. Acontece quando um incidente se prolonga para além de um período predefinido.
Desastre	Acontecimento imprevisto e calamitoso que origina perdas e dificuldades à totalidade ou a parte da Empresa, com um impacto negativo significativo sobre a sua capacidade para executar serviços essenciais por um determinado período de tempo.
Detecção (capacidade de)	Visibilidade sobre a concretização das ameaças.
Disponibilidade	Acessibilidade a um determinado elemento (informação, instalações, sistemas, etc.)
Emergência	Período normalmente reduzido em que decorre um acontecimento imprevisto e calamitoso.

Função de negócio	Função estratégica do negócio, suportada por processos e actividades; o primeiro nível da Cadeia de Valor de Porter. Exemplos de função: marketing, distribuição, etc.
Gestor da Continuidade do Negócio	Responsável pela definição, manutenção, divulgação e teste do Plano de Continuidade do Negócio.
Impacto	Resultado da concretização de uma ameaça que explore com sucesso uma vulnerabilidade existente.
Inspecção (capacidade de)	Característica conferida por um conjunto de medidas que possibilitam a análise dos eventos ocorridos.
Integridade	Característica da informação que não sofreu quebra de confidencialidade ou modificação.
Invocação	Ver “Activação”.
Milestones	Momentos chave.
NFM	Necessidade de fundo de maneio: necessidade de fluxos de caixa por um determinado período.
PCN	*Business Continuity Plan*: ver “Plano de Continuidade do Negócio”
Plano de Contingência	Documento detalhando as actividades de contenção de desastre a realizar durante a fase de contingência.

Plano de Continuidade do Negócio	Documento detalhando todos os procedimentos a implementar e os recursos humanos, técnicos e materiais necessários à sua concretização em caso de desastre, por forma a permitir ao negócio a continuação da sua actividade (degradação graciosa). Este documento pode ser sub-dividido em planos de contingência, de recuperação e de gestão de crise.
Plano de Recuperação de Desastre	Documento detalhando o processo de recuperação da capacidade de realização das funções críticas, a realizar durante o período de recuperação de desastre.
Prazo alvo (para a recuperação)	*Recovery Time Objective* – RTO: o prazo pretendido para a recuperação de determinada função, processo ou actividade de negócio.
PRD	Plano de Recuperação de Desastre: ver "Plano de Recuperação de Desastre"
Prevenção	Conjunto de actividades destinadas a reduzir a probabilidade de ocorrência de um desastre.
Probabilidade	Número médio expectável de vezes que uma determinada ameaça se possa concretizar num determinado período.
Processo do negócio	Componente de uma função de negócio constituído por diversas actividades de suporte; o segundo nível da Cadeia de Valor de Porter.

Programa	Conjunto de projectos e outras actividades que visam atingir determinado objectivo concreto; possui um âmbito mais alargado e uma complexidade e duração superiores a um projecto.
Projecto	Conjunto de actividades que visam um objectivo concreto, com uma duração limitada e finita.
Protecção	Actividades destinadas a reduzir o impacto de um desastre.
Reacção (capacidade de)	Característica conferida por um conjunto de medidas que permitem responder activamente a eventos.
Recuperação	Capacidade de retoma das actividades e processos de suporte às funções do negócio.
Reflexo (capacidade de)	Característica conferida por um conjunto de medidas que possibilitam uma reacção automática a um estímulo externo.
Repúdio	Rejeição voluntária da autoria de um determinado acto.
Risco	Exposição a uma determinada ameaça.
SI	Sistemas de informação.
SLA	*Service Level Agreement*: acordo de nível de serviço.
SWOT	*Strenghts, weaknesses, opportunities and threats*: Pontos fortes, pontos fracos, oportunidades e ameaças
TAR	Tempo alvo de recuperação.

TI	Tecnologias de informação.
Vulnerabilidade	Característica que potencia o impacto da concretização de determinada ameaça.

Bibliografia

ATKINSON, Anthony A., Management Accounting, Prentice-Hall, Nova Jersey, 1997

BLAKLEY, B., "The Emperor's Old Armour", in: Proceedings of the New Security Paradigms Workshop, IEEE Computer Society Press, 1996

BRINK, Derek, "PKI and Financial Return on Investment", in: White Paper, PKI Forum's Business Working Group, Agosto de 2002

Carnegie Mellon Computer Emergency Response Team, CERT Advisory CA-2001: Unauthentic "Microsoft Corporation" Certificates, 22 de Março de 2001

Carnegie Mellon Computer Emergency Response Team, Survivable Systems Analysis Method, CERT, http://www.cert.org/archive/html/ analysis-method.html, 2002

Computer Security Institute / Federal Bureau of Investigation, 2002 CSI/FBI Computer Crime and Security Survey, 2002

Disaster Recovery Institute International, Professional Practices for Business Continuity Planners, DRII, Disaster Recovery Institute International, 2001

ELLIS, Juanita e SPEED, Timothy, The Internet Security Guidebook: From Planning to Deployment, Academic Press, USA, 2001

ELLISON, Carl e SCHNEIER, Bruce, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", in: Computer Security Journal, Volume XVI, Nº 1, 2000

GOLLMANN, Dieter, Computer Security, Wiley, USA, 2000

HALLAWELL, A., PESCATORE, J., Signature-Based Virus Detection at the Desktop Is Dying, Gartner Research, 31 de Agosto de 2001

HALLIDAY, S., ADENHORST, K., Solms, R., "A Business Approach to Effective Information Technology Risk Analysis and Management", in: Information Management & Computer Security, pp. 19-31, MCB University Press, 1996

International Standards Organization, International Standard ISO/IEC 17799: Information Technology – Code of practice for information security management, s.e., Genebra, 2000

KIRAN, Shashi, LAREAU, Patricia, LLOYD, Steve, PKI Basics – A Technical Perspective, PKI Forum's Business Working Group, Novembro de 2002

KOTTER, John P., A Force for Change: How leadership differs from management, The Free Press, Nova Iorque, 1990

KOTTER, John P., Leading Change, Harvard Business School Press, 1996

LIPSON, H. F., FISHER, D. A., "Survivability – A New Technical and Business Perspective on Security", in: Proceedings of the New Security Paradigms Workshop, IEEE Computer Society Press, 1999

PARRISH, Scott, Security Considerations for Enterprise Level Backups, SANS Institute, 2001

PELTIER, Thomas R., Information Security Risk Analysis, Auerbach, USA, 2001

PIPKIN, Donald L., Information Security, Prentice Hall, USA, 2000

S.A., What's New in Security for Windows XP Professional and Windows XP Home Edition, Microsoft Corporation, Julho de 2001

SCHNEIER, Bruce, "Fun with Fingerprint Readers", in: Crypto-Gram Newsletter, nº 25, s.l., 15 de Maio de 2002

SCHNEIER, Bruce, "Kerberos and Windows 2000", in: Crypto-Gram Newsletter, s.n.º, s.l., 15 de Março de 2000

SCHNEIER, Bruce, Applied Cryptography – Protocols, Algortihms and Source Code in C, John Wiley & Sons, Nova Iorque, 1996 (2ª ed.)

SCHNEIER, Bruce, Secrets And Lies: Digital Security in a Networked World, John Wiley & Sons, Nova Iorque, 2000

SCHUCHART JR., Steven J., "Restoring SANity", in: Network Computing, Janeiro de 1997

SILVA, Pedro T. e CARVALHO, Hugo, "Análise de Risco e Definição de Políticas de Armazenamento no Ciclo de Vida da Continuidade do Negócio", in: Terceiro Encontro de Segurança dos Sistemas de Informação, IFE - International Faculty for Executives, Lisboa, 2002

THOMPSON, Herbert H. e WHITTAKER, James A., "Testing for Software Security", in: Dr. Dobb's Journal, nº 342, Novembro de 2002

TOIGO, Jon William, Disaster Recovery Planning, Prentice Hall, 2000 (2ª ed.)

TRIMMER, Don, "Tape-free backup/recovery: Requirements and Advantages", in: Infostor, Março de 2002

VV.AA., Model-based Risk Management Using UML and UP, CORAS/Directorate-General Informatin Society, s.l., s.d.

WHEATMAN, V. e PESCATORE, J., The Information Security Hype Cycle, Gartner Research, 15 de Novembro de 2001

WROZEK, Brian, Electronic Data Retention Policy, SANS Institute, s.l., 2001

ZIMMERMANN, Phil, "Security Features and Vulnerabilities", in: PGP-INTRO/PGP User Manual, s.l., s.d.